与众不同的合规理念：
低成本、高效率、高价值

We Are Making a Difference:
Compliance with Low-cost &
High-efficiency & High-value.

《企业内部控制基本规范》合规实务指南

梁晟耀 编著



《企业内部控制基本规范》
合规实务指南

随着《企业内部控制基本规范》的实施，国内企业面临内控合规的严峻考验。

本书立足于当下中国企业实务与实践，详细介绍了企业内部控制体系建设的全过程，并分享了很多企业在此过程中的经验与教训。提高效率，减少成本，从合规中提升价值，是本书的目的之所在。

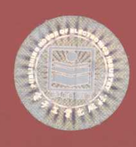
建立与实施有效的内部控制，一方面，有利于改进公司治理，优化营运流程，改善控制措施，降低风险不良影响，并提高企业运作透明度，另一方面，有利于增强投资者和市场对企业的信心，提高企业的凝聚力、员工的士气和自豪感。

世纪波文化发展有限公司
http://www.century-wave.com



咨询投稿：(010) 88254199
sjb@phei.com.cn

责任编辑：王慧丽





ISBN 978-7-121-10652-1

定价：48.00元

《企业内部控制基本规范》合规实务指南

梁晟耀◎编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

图书在版编目（CIP）数据

《企业内部控制基本规范》合规实务指南/梁晟耀编著. —北京：电子工业出版社，2010.4
ISBN 978-7-121-10652-1

Ⅰ. ①企… Ⅱ. ①梁… Ⅲ. ①企业管理－内部审计－规范－基本知识－中国
Ⅳ. ①F239.45-65

中国版本图书馆 CIP 数据核字（2010）第 058231 号

策划编辑：王慧丽
责任编辑：王慧丽
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1000　1/16　印张：18.5　字数：247 千字
印　　次：2010 年 4 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

推荐序

公司基业长青的内部控制指南

前段时间，曾与一位投资银行的朋友探讨尽职调查，其言工作中曾涉及一些内部控制的相关内容，由于专业知识等方面的局限，往往流于形式而仅能实现“纸上合规”。恰巧此时，有幸拜读梁晟耀先生所编著的《<企业内部控制基本规范>合规实务指南》书稿。该书不仅可解朋友之惑，也使自己受益匪浅。

之于内部控制，往往存在以下两种有些对立的认知。

一是认为内部控制只是会计分工、内部牵制等方面内容，属公司财务部门的自娱自乐，或者是财务部门与其他部门的协调配合。其实，目前内部控制理论与实践已得到极大发展，已经历五个阶段，从初级的“内部牵制”发展至第五阶段的“企业风险管理整合框架”。

尽管更侧重于实务层面，但梁晟耀先生也在书中对内部控制理论进行了梳理概括，在介绍美国内部控制理论和实践发展的基础上，重点讨论了

我国的情况。

没有理论指导的实践是盲目的。书中讲述的内部控制理论可谓恰到好处，能够使读者茅塞顿开，进而从更宏观的层面了解和理解内部控制的发展历程与概念内核，以便更精准地指导实践。

二是言及内部控制则肃然起敬，复杂理论与烦琐规则不绝于口，置人于云雾之中。其实，内部控制并非深不可测，它只是人们在经营管理实践中的一种科学总结，也可以从几个要素来把握，如控制环境、风险评估、控制活动、信息与沟通及监控。

真知往往存在于实践之中。内部控制实务则是梁晟耀先生这本书的重头戏，也是能够答疑解惑的关键所在。甚至，更见体贴入微之处的是，在内部控制与全面风险管理体系建设方案的探讨里，提出了一些技巧性的具体做法。

例如，在《企业内部控制基本规范》合规的头一年，建议采用项目管理办公室的办法，在董事会及审计委员会的领导下，由公司高层担任“内部控制建设项目”负责人，在其领导下成立“内部控制建设项目指导委员会”，全面负责协调整个项目的顺利实施；又如，对于大型企业，下属公司繁多，可以采取先试点、后推广的方法。

其实，梁晟耀先生对书稿内容的定位是煞费苦心的。内部控制往往涉及方面众多，而基本规范则是最基础的，纲举目张，只有基础打牢了，才能成就内部控制的屹立百年的高楼大厦。同时，由于目前我国企业规模与发展阶段的局限，经营管理往往缺乏主动性。这样，以合规这一基础性要求为第一要务，不仅能够使企业更快地切入内部控制建设上来，也有可能在实践过程中逐渐认识内部控制的重要性，进而上升到更高层次的主动性管理。

企业内部控制做不好就不能基业长青。这不仅仅局限于中大型公司或上市公司，众多民营中小企业也同样如此。企业在内部控制构建中，需把握其核心理念——风险管理。大公司面临风险，中小企业更面临风险。风险管理的理念贯彻于本书中，与此相应，书中将风险评估作为单独一章来专门阐释，足见其充分的内在逻辑。

如果说内部控制体系建设工作应贯彻于企业始终的话，那么对内部控制理论与实践的思考也将成为梁晟耀先生一生的追求。期待梁晟耀先生未来能有更多的如本书般有价值的优秀作品，也期待能有更多鲜活生动的案例与广大读者分享。

拙以为，梁晟耀先生书中所探讨的，不仅仅利于广大企业进行内部控制制度建设实践，也是上市公司合规经营的指导手册，更值得证券界、审计界及学界等各方面借鉴。喜读之余，乐于推荐。

王大力

西南证券研究发展中心

郑朝晖

华泰联合证券有限责任公司

2010 年 3 月

前 言

狄更斯在其《双城记》的开头说："这是最好的时代，这是最坏的时代。"（It was the best of times, it was the worst of times.）时至今日，这个世界从来没有平静过。

2001 年 11 月至 2002 年 6 月，美国发生了被称为经济界"9·11"事件的安然、世通等公司的财务欺诈丑闻，催生了 2002 年《萨班斯法案》，开启了全球内控时代。

2010 年 3 月 11 日，雷曼兄弟倒闭一年半之后，关于该公司倒闭事件的调查报告出炉，结果说明其采取了与安然如出一辙的高达数百亿美元的会计作假行为，报告指出其"内控和会计程序极不完善"（where control and accounting procedures were found to be sorely lacking.），《萨班斯法案》没能防止美国第二个安然式的会计丑闻的出现。

而在中国，这些年来，黑煤窑和毒奶粉给我们带来的伤痛还没有远去……

2008 年 6 月 28 日，财政部、证监会、审计署、银监会、保监会五部委联合发布了《企业内部控制基本规范》。中国版萨班斯自此诞生，成为中国内部控制的一个标志性里程碑。

王石说："这真是一个荒唐的年代。"在中国做企业，如果你能真的做到以下几点，就是一个优秀的时代标杆了。这些品质是：不向官员行贿，不偷税漏税，不拖欠员工工资，不违反标准排放污水毒气，没有往产品里掺"三聚氰胺"。

人类的理性是有限的。在这样一个充满复杂性的年代，人类预测未来的知识瞬间显得苍白。企业亦然，在瞬息万变的经营环境中，往往手足无措。符合内部控制监管合规要求仅是企业内部控制体系建设的初级阶段。将内部控制植根于企业运营，融入企业文化，才是更务实的选择。

2006 年，笔者创建了国内唯一专注于内部控制与全面风险管理的网站 **Cosox**（www.cosox.cn）。通过这个平台，我结识了许多业内同行。通过与他们的交流，我对中国企业的内部控制有了更深入的理解和认识。

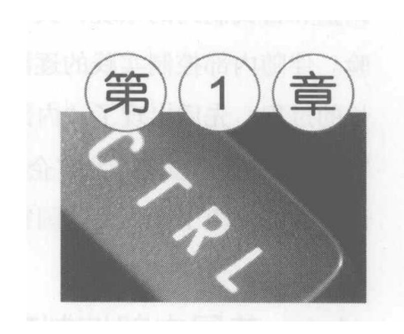
本书的出版，得到了很多人的支持。特别感谢江湖号称"财务杀手"的郑朝晖（笔名夏草/飞草）和西南证券研究发展中心王大力两位前辈于百忙之中为本书作序，使本书增色不少。同时，还要感谢我的太太，她在我需要鼓励时给了我勇气，并悉心照顾家庭，使我有足够的时间来完成本书。

谨以此书献给我深爱的母亲粟连玉！

梁晟耀

2010 年 2 月

目 录



《企业内部控制基本规范》解读

现代意义上的企业内部控制是在长期的经营活动过程中，随着企业对内加强管理和对外满足社会需要，逐渐产生并发展起来的自我检查、自我调整和自我制约的系统，其中凝聚着诸多的经济思想、管理理论和实践经验。伴随内部控制实践的逐渐丰富，内部控制理论的发展也经历了一个漫长的过程，先后出现了“内部牵制”、“内部控制制度”、“内部控制结构”、“内部控制整合框架”和“企业风险管理整合框架”五个阶段。内部控制理论与实践起源于西方发达国家，特别是美国。

1.1 美国内部控制理论和实践的发展

1992 年，由美国注册会计师协会（AICPA）、美国会计学会（AAA）、财务经理人协会（FEI）、国际内部审计师协会（IIA）和管理会计师协会（IMA）共同赞助成立的一个专门研究内部控制的问题委员会——COSO 委员会（Committee of Sponsoring Organizations of the Treadway Commission，全美反舞弊性财务报告委员会发起组织），发布了指导内部控制实践的纲领性文件 COSO 研究报告：《内部控制——整合框架》。该框架是至今管理当局和注册会计师在财务呈报内部控制有效性评价方面的依据之一。在 COSO 报告中，内部控制被定义为一个受企业员工行为影响，用以完成特定目标的过程。内部控制是一个受到董事会、管理层和其他人员影响的过程，该过程的设计是为了提供实现以下三类目标的合理保证：经营的效果和效率、财务报告的可靠性、法律法规的遵循性。内部控制包括控制环境、风险评估、控制活动、信息与沟通、监控五个相互联系的要素，它们都包含在管理层经营企业的方式中。五项要素相互联系，作为评判内部控制系统是否有效的准则。

2002年，安然、世通公司突然垮台，施乐、默克等美国一系列大型企业相继出现财务丑闻，为整个金融市场敲响了警钟。这些丑闻的出现，不是偶然事件，与其对内部控制的过分疏忽有密切的关系。继这些丑闻曝光后，2002年7月30日，美国紧急出台了著名的《2002年公众公司会计改革和投资者保护法案》，又被称做2002年《萨班斯—奥克斯利法案》（简称《萨班斯法案》，SOX），同时成立了一个新的监管机构——上市公司会计监督委员会（The Public Company Accounting Oversight Board，PCAOB）取代美国注册会计师协会来监管会计职业界。该法案是1930年以来美国证券立法中最具影响的法案，它加重了公司主要管理者的法律责任，加强了对公司高级管理层的收入监管，对公司内部的审计委员会做出了法律规范；与此同时，该法案强化了对公司外部审计的监管，加强了信息披露制度和其他有关公司监管的规定。

《萨班斯法案》的影响已波及整个资本市场，各行各业都受到并将继续受到该法案的影响。该法案中的404条款管理层对内部控制的评估是最棘手的部分，它要求上市公司及其外部审计师对公司财务报告内部控制的有效性进行报告。

在《萨班斯法案》颁布之后，COSO委员会于2004年9月29日正式发布了《企业风险管理——整合框架》，并提出由此取代《内部控制——整合框架》（见图1-1）。《企业风险管理——整合框架》内部控制标准体系是公司内部管理当局与外部注册会计师完成财务呈报内部控制有效性评价的标准。

COSO委员会提出，企业风险管理是企业的董事会、管理层和其他员工共同参与的一个过程，应用于企业的战略制定和企业的各个部门和各项经营活动，用于确认可能影响企业的潜在事项并在其风险偏好范围内管理

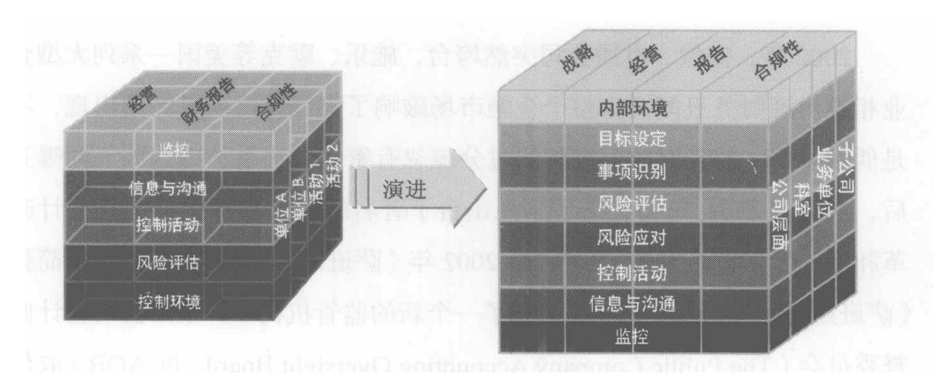


图 1-1　COSO-IC 演进到 COSO-ERM

风险，对企业目标的实现提供合理的保证。根据管理者经营的方式划分，企业风险管理包括八个相互关联的组成要素：内部环境、目标设定、事项识别、风险评估、风险应对、控制活动、信息与沟通和监控。内部环境是企业风险管理的基础，为企业风险管理所有其他组成部分的运行提供了平台和结构。企业风险管理的八个组成部分体现的是一个动态的过程，是一个有机的整体。

《内部控制——整合框架》到《企业风险管理——整合框架》，不是局部的修补和简单改良，而是在理念上的本质突破。体现在：从“控制环境”到“内部环境”，这一修改使得企业关注的范围不再局限于控制方面，而是从更宽阔的视野，更综合、更直接地考虑各种因素对风险的影响；目标设定中增加“战略目标”，使企业在追求短期利益的同时，从战略的高度关注企业的长远目标和可持续发展；将“风险评估”扩展为“事项识别”、“风险评估”和“风险应对”，不是对原“风险评估”进行简单的细化，而是代表着企业风险意识日益增强和积极主动管理风险。美国上市公司监管机构推出的一系列针对内部控制的制度安排，对我国在美国上市公司具有直接影响，对我国市场监管也具有借鉴意义。

1.2 我国内部控制理论和实践的发展

1.2.1 我国内部控制发展脉络

2007年3月，企业内部控制标准委员会颁布《企业内部控制规范——基本规范》和17项具体规范（征求意见稿），向社会公开征求意见，标志着我国内部控制标准制定工作正式起航。在此之前，我国已经出台了一系列内部控制相关规范，如表1-1所示。

表1-1 我国内部控制规范进程一览表

序号	时　间	发布部门	规范内容
1	1996年12月	财政部	发布《独立审计具体准则第9号——内部控制与审计风险》
2	1997年5月	中国人民银行	发布《关于加强金融机构内部控制的指导原则》，这是我国第一个关于内部控制的行政规定
	2002年9月		发布《商业银行内部控制指引》，取代1997年5月发布的《关于加强金融机构内部控制的指导原则》，旨在促进商业银行建立和健全内部控制体系，防范金融风险，保障银行体系安全稳健运行
3	1999年6月	证监会	发布《关于上市公司做好各项资产减值准备等有关事项的通知》，开始要求上市公司建立内部控制
4	2000年11月	证监会	发布《公开发行证券公司信息披露编报规则》，要求商业银行、保险公司、证券公司必须建立健全内部控制，并对内部控制的完整性、合理性和有效性做出说明
5	2000年7月	全国人大	发布《会计学》，首次以法律的形式对企业的内部控制做出相应的规定，将其纳入企业内部会计监督制度

续表

序号	时　间	发布部门	规范内容
6	2001年2月	证监会	发布《证券公司内部控制指引》，要求证券公司健全内部控制机制，完善内部控制，以规范公司经营行为；要求证券公司应当按照指引的要求，建立运行高效、科学合理、切实有效的内部控制
	2003年12月		发布《证券公司内部控制指引》修订版，引导证券公司规范经营，完善内部控制机制，增强自我约束能力，推动现代企业制度建设，防范和化解金融风险
7	2001年6月	财政部	发布《内部会计控制规范——基本规范（试行）》和《内部会计控制规范——货币资金（试行）》
8	2002年3月	中注协	发布《内部控制审核指导意见》，规范注册会计师执行内部控制审核业务，明确工作要求，保证执业质量
9	2002年12月	财政部	发布《内部会计控制规范——采购与付款（试行）》和《内部会计控制规范——销售与收款（试行）》
10	2003年11月	财政部	发布《内部会计控制规范——存货（试行）》《内部会计控制规范——担保（征求意见稿）》和《内部会计控制规范——成本费用（征求意见稿）》
11	2004年12月	银监会	发布《商业银行内部控制评价试行办法》，为规范和加强对商业银行内部控制的评价，建立健全内部控制机制，为全面风险管理体系的建立奠定基础，保证商业银行安全稳健运行
12	2005年10月	国务院证监会	发布《关于提高上市公司质量意见》，国务院首次就上市公司工作批转发布文件
13	2006年1月	保监会	发布《寿险公司内部控制评价办法（试行）》，规范和加强对寿险公司内部控制的评价，推动寿险公司加强内部控制建设
14	2006年5月	深交所	发布征求《上市公司内部控制指引》意见的通知，揭开了中国上市公司内部控制体系制度建设的序幕
15	2006年5月	证监会	发布《首次公开发行股票并上市管理办法》第29条规定，发行人有CPA出具的无保留的内部控制报告，证监会首次对上市公司内部控制提出具体要求

续表

序号	时　间	发布部门	规范内容
16	2006年6月	上交所	发布《上海证券交易所上市公司内部控制指引》
17	2006年6月	国资委	发布《中央企业全面风险管理指引》
18	2006年7月	财政部	发起成立“企业内部控制标准委员会”
19	2006年7月	中注协	发起成立“会计师事务所内部治理指导委员会”
20	2006年9月	深交所	发布《深圳证券交易所上市公司内部控制指引》，规定2007年6月30日前，深市主板上市公司均要按要求披露内部控制制度的制定和实施情况

通过表1-1，我们不难发现，从1996年到2006年总共颁布了20项与内部控制相关的法律法规，特别是在2006年，共出台了8个与内部控制相关的法规，并成立了2个与内部控制相关的委员会。可以想见，这一连串法规的出台或多或少都与《萨班斯法案》有关，因为《萨班斯法案》是2002年颁布的，从2006年7月15日开始，所有在美国上市的外国企业（包括中国在美国上市公司），必须执行《萨班斯法案》，这意味着中国在美国上市公司的内部控制建设直接受到美国法律的约束。

1.2.2　财政部《企业内部控制基本规范》

1. 背景

2006年7月15日，财政部发起成立了企业内部控制标准委员会，负责建立一套以防范风险和控制舞弊为中心、以控制标准和评价标准为主体，结构合理、内容完整、方法科学的内部控制标准体系，推动企业完善治理结构和内部约束机制。

2007年3月，企业内部控制标准委员会颁布《企业内部控制规范——基本规范》和17项具体规范（征求意见稿），向社会公开征求意见。

2008年6月28日，财政部、证监会、审计署、银监会、保监会联合发布《企业内部控制基本规范》(以下简称《内控规范》)，标志中国版萨班斯（C-SOX）正式亮相，自此中国有了自己统一的内部控制标准。此前，上海证券交易所、深圳证券交易所、中国证券监督管理委员会都分别出台过关于上市公司内部控制的相关指导意见，但这些要求之间或多或少地存在不一致性。

《内控规范》的发布是中国在公司治理方面的一个重要里程碑，体现了中国经济与全球经济的进一步接轨和融合。随着中国资本市场的发展与壮大，与之配套的公司治理和监督机制的需求日益增加；而随着中国企业的做大做强，企业对于内部外部的风险需要更有系统、更有力的控制。《内控规范》为中国企业建立内部控制体系提供了一个标准的框架，在理念、实施和制度层面为企业提供了基础。同时，内部控制作为一个相对较新的课题对首次系统建立与实施内部控制体系的企业提出了新的挑战。

相关链接

理解《内控规范》注意事项

- 2008年6月28日，财政部、审计署、证监会、银监会、保监会联合颁布了《内控规范》，但正式官方文件于2008年5月22日以通知形式下发，即“关于印发《内控规范》的通知”财会[2008]7号（以下简称《通知》)。理解《内控规范》时不能仅仅看《内控规范》本身，也需考虑《通知》中的相关要求。
- 《通知》要求自2009年7月1日起在上市公司范围内施行，鼓励非上市的大中型企业执行。执行本规范的上市公司，应当对本公司内部控制的有效性进行自我评价，披露年度自我评价报告，并可聘请具有证券、期货业务资格的会计师事务所对内部控制的有

效性进行审计。

来源：财政部网站 http://www.casc.gov.cn/gnxw/200 807/t20 080 715 751 587.htm

2.《内控规范》简介

（1）框架

《内控规范》基本借鉴了美国 COSO 框架，即以 1992 年 COSO《内部控制——整合框架》五要素为框架，同时在内容上体现了 2004 年 COSO《企业风险管理——整合框架》八要素框架的实质。

从目标上看，《内控规范》（第三条）融合了 1992 年 COSO《内部控制——整合框架》和 2004 年 COSO《企业风险管理——整合框架》的目标：

① 发展战略。

② 经营效率和效果。

③ 财务报告及相关信息真实完整。

④ 资产安全。

⑤ 经营管理合法合规。

（2）结构

《内控规范》的结构如图 1-2 所示。

《内控规范》共分为七章五十条：

① 第一章定义基本规范的适用范围，提出了管理层年度评估内部控制的要求。

② 第二～六章叙述企业内部控制需要考虑的原则与相关管理要素，包括内部环境、风险评估、控制活动、信息与沟通和内部监督。

③ 第七章规定基本规范开始实施的日期，指明了规范的配套办法将由相关部门另行制定。

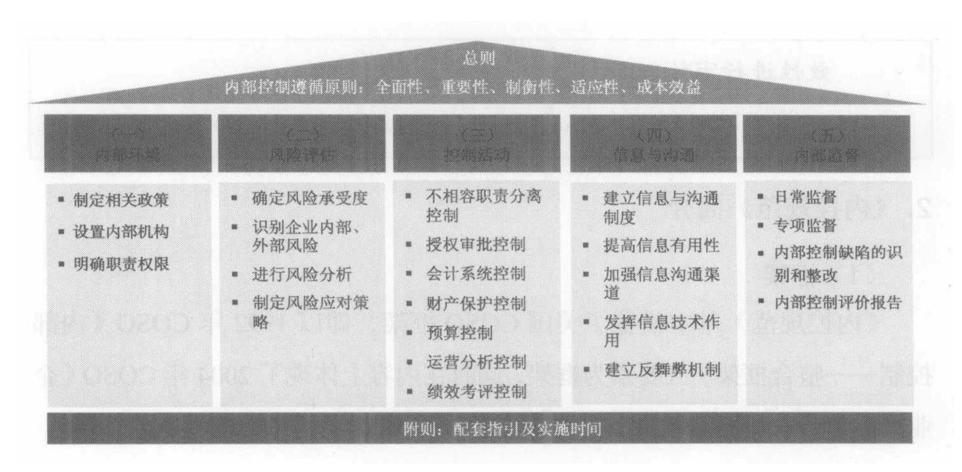


图 1-2　《内控规范》的结构


相关链接

《内控规范》的特色

- 《内控规范》包含了全部控制要素，没有如《萨班斯法案》仅仅局限于财务报告相关的内部控制（Internal control over financial reporting，ICFR），其范围更为广泛，因此与《萨班斯法案》等内部控制法规不尽相同。
- 《内控规范》第八条要求企业建立内部控制实施的激励约束机制，将各责任单位和全体员工实施内部控制的情况纳入绩效考评体系，促进内部控制的有效实施。

（3）审计师的考虑

1）不强制要求独立审计

可聘请具有证券、期货业务资格的会计师事务所对内部控制的有效性进行审计（《通知》）。

2）审计标准

必须按照基本规范、支持性的法规和相关专业指引要求执行审计（《内

控规范》第十二条)。

3）审计师的资质

具有证券、期货业务资格的会计师事务所(《通知》)。

4）独立性要求

提供内部控制咨询服务的公司不能同时提供内部控制审计服务(《内控规范》第十二条)。

1.2.3 我国内部控制体系进展

1. 配套指引

《内控规范》发布后，为了配合其施行，2008年7月4日，官方[①]发布了“关于征求《企业内部控制评价指引》、《企业内部控制应用指引》和《企业内部控制鉴证指引》意见的通知”。至此，我国的企业内部控制法规体系初步形成一个层次分明、内容完整、衔接有序、整体互动的有机统一体。

（1）《企业内部控制评价指引》

由财政部制定，用于指导企业管理层对内部控制有效性进行年度评价，包括内部控制评价的程序和方法、缺陷认定和评价报告。

（2）《企业内部控制应用指引》

由财政部制定，用于指导企业管理层实施内部控制。该指引设置了22个独立文件，覆盖的领域包括资金、采购、存货、销售、工程项目、固定资产、无形资产、长期股权投资、筹资、预算、成本费用、担保、合同协议、对子公司的控制、财务报告编制与披露、人力资源政策、信息系统一

① 《企业内部控制基本规范》的配套指引是通过“企业内部控制标准委员会”秘书处即财政部会计司的网站来发布的。

般控制、衍生工具、企业并购、关联交易、业务外包和内部审计。

（3）《企业内部控制鉴证指引》

由中国注册会计师协会制定，用于指导接受企业委托从事内部控制审计的会计师事务所，从事企业内部控制有效性鉴证业务。目前指引将范围限定在有关财务报告相关的内部控制，小于《内控规范》中规定的内部控制范围。

2. 配套指引进展

（1）根据官方公布的消息，配套指引的进展情况

① 《企业内部控制评价指引》。2009 年 1 月 14 日，修改了《企业内部控制评价指引》（财会便[2009] 7 号）（参考附录 A）。

② 《企业内部控制应用指引》。根据目前官方公布的信息，已经做了如下一些修订：

- 2008 年 12 月 31 日，新增了组织架构、发展战略、人力资源、企业文化和社会责任 5 个项目（财会便[2008] 60 号）。
- 2009 年 1 月 8 日，调整修改了资金、采购、资产、销售、研发 5 个应用指引（财会便[2009] 4 号）。
- 2009 年 1 月 14 日，调整修改了工程项目、全面预算、合同、内部报告、信息系统 5 个应用指引（财会便[2009] 7 号）。

③ 《企业内部控制鉴证指引》。没有看到关于这个指引的修订信息。

（2）除了官方正式公布消息外，其他渠道透露的消息

2009 年 2 月，财政部会计司拟稿了一套《企业内部控制配套指引》（征求意见稿）。该配套指引包括三部分内容：18 项应用指引、1 项评价指引和 1 项审计指引。《企业内部控制应用指引》包括组织架构、发展战略、人力

资源、企业文化、社会责任、资金、采购、资产、销售、研发、工程项目、全面预算、合同、内部报告、信息系统、银行业务、保险业务、证券业务 18 项;《企业内部控制评价指引》就是 2009 年 1 月 14 日修改后的版本(参考附录 A);《企业内部控制审计指引》取代之前发布的《企业内部控制鉴证指引》(参考附录 B)。

相关链接

《内控规范》配套指引进展

- 2009 年 7 月 22 日，在《中国会计报》创刊一周年暨首届中国财会论坛上，财政部副部长王军表示，在业已发布《内控规范》的基础上，财政部制定完成了 18 项应用指引、1 项评价指引和 1 项审计指引，并提交证监会、审计署、银监会、保监会会签，将于近期正式公布。

来源：中国证券网 http://www.cnstock.com/08index/2009-07/22/content_4 451 022.htm

- 2009 年 9 月 10 日，美国管理会计师协会在上海召开第四届全球年会，中国财政部会计司副司长李玉环在该会上表示，在已发布《内控规范》的基础上，目前财政部已经完成了 18 项应用指引、1 项评价指引和 1 项审计指引，并会签证监会、审计署、银监会、保监会，具体内容不久后即将公布。

来源:《国际金融报》

从 2007 年 3 月，企业内部控制标准委员会颁布《企业内部控制规范——基本规范》和 17 项具体规范(征求意见稿)，到目前《内控规范》的配套指引即将发布，我国企业内部控制规范及其配套指引发展演变如表 1-2 所示。

表 1-2 内部控制规范配套指引发展演变（2007—2009）[①]

2007 年	2008 年	2009 年
–	《企业内部控制评价指引》（征求意见稿）	《企业内部控制评价指引》（修订版）
–	《企业内部控制鉴证指引》（征求意见稿）	《企业内部控制审计指引》（修订版）
《企业内部控制具体规范》（2007 年征求意见稿）17 项	《企业内部控制应用指引》（2008 年征求意见稿）22 项	《企业内部控制应用指引》（最新修订稿意见稿）18 项
• 货币资金 • 采购与付款 • 存货 • 对外投资 • 工程项目 • 固定资产 • 销售与收款 • 筹资 • 成本费用 • 担保 • 财务会计报告编制 • 信息披露 • 预算 • 合同 • 对子公司的控制 • 人力资源政策 • 计算机信息系统	• 资金 • 采购 • 存货 • 销售 • 工程项目 • 固定资产 • 长期股权投资 • 筹资 • 预算 • 成本费用 • 担保 • 合同协议 • 对子公司的控制 • 人力资源政策 • 信息系统一般控制 • 财务报告编制与披露 • 无形资产 • 衍生工具 • 企业并购 • 关联交易 • 内部审计 • 业务外包	• 组织架构 • 发展战略 • 人力资源 • 企业文化 • 社会责任 • 资金 • 采购 • 资产 • 销售 • 研发 • 工程项目 • 全面预算 • 合同 • 内部报告 • 信息系统 • 银行业务 • 保险业务 • 证券业务

① 请以最终公布版为准。

等到《内控规范》的配套指引发布正式稿，中国内部控制标准体系将正式形成，如图1-3所示。

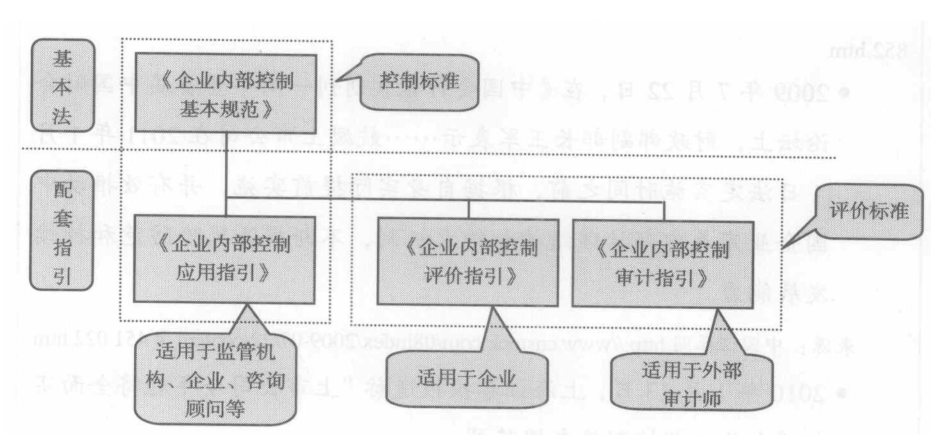


图1-3　中国内部控制标准体系

3．实施时间

《内控规范》第五十条："本规范自2009年7月1日起实施。"但是目前对于实施时间的说法有很多版本，众说纷纭。

相关链接

《内控规范》实施时间新闻报道

- 2009年5月9日《中国经营报》刊发一篇报道：《中国版<萨班斯法案>延期》，没有任何预兆，也没有任何公示，财政部悄然推后了《内控规范》实施的时间，从2009年7月1日延期到2010年1月1日开始施行。

来源：《中国经营报》http://news.cb.com.cn/html/37/n-6 537.html

- 2009年7月1日《新京报》报道：被喻为中国《萨班斯法案》的《内控规范》今起实施。财政部会计司相关工作人员昨日表示，截

至昨日下午，没有正式文件或正式说法说《内控规范》延期执行。

来源：《新京报》http://www.thebeijingnews.com/economy/2009/07-01/008@021852.htm

- 2009 年 7 月 22 日，在《中国会计报》创刊一周年暨首届中国财会论坛上，财政部副部长王军表示……鼓励上市公司在 2011 年 1 月 1 日法定实施时间之前，根据自身实际提前实施，并有效推动中国企业完善内部治理结构和约束机制，不断提高风险防范和持续发展能力。

来源：中国证券网 http://www.cnstock.com/08index/2009-07/22/content_4 451 022.htm

- 2010 年 1 月 13 日，上海证券报报道称“上市公司今年起将全面实行《企业内部控制基本规范》”。

来源：上海证券报 http://www.stockinfo.com.cn/paper_new/html/2010-01/13/content_71930107.htm

《内控规范》延期的一个很重要原因是对执行成本的考虑。内部控制需要对企业业务流程进行梳理，增设专门的部门，配备专业人员，甚至需要聘请咨询公司，这都是一笔不小的开支。当前金融危机情况下，很多企业的业绩大受影响，适当延期实施《内控规范》乃应景为之。

从美国实施《萨班斯法案》的经验来看，需要考虑到实施中可能出现一些困难，如一些企业可能会由于时间有限而使实施流于形式，或在短期内无法完成内部控制的建设工作，为了避免这些情况，保证实施的效果，《萨班斯法案》的实施也是将实施范围内的公司分为几个类别，并分别数次推迟了这几类公司正式实施的时间。因此《内控规范》实施或多或少受到《萨班斯方案》实施过程所遇到的情况的影响。



相关链接

《萨班斯法案》的境遇

- 《萨班斯法案》实施争议不断，被认为成本高昂，价值有限，甚至认为其严重影响了美国资本市场的竞争力。

来源：中注协行业发展研究资料（No.2007—2）:《萨班斯法案》404条款实施的跟踪研究——各方评论、实施进展与启示

（http://www.cicpa.org.cn/Column/Research_data/200 805/t20 080 530_12 804.htm）

- 2009年10月2日美国证券交易委员会（Securities and Exchange Commission，SEC）再次宣布将小规模报告公司（流通在外的由公众持有的股份市值低于USD75M）的合规日期延迟至2010年6月15日之后。也就是那时之后才需要外部审计师须就公司的财务报告内部控制的有效性出具审计意见。这是SEC第四次也是最后一次推迟小型上市公司遵守《萨班斯法案》404（b）条款的日期。

来源：美国证交会

1.3 内部控制的规定及相关人员的责任

1.3.1 相关法规对内部控制的规定

国内外近几年颁布的有关内部控制的法律法规，均做出了具体的规定。

1．我国相关法规对企业建立内部控制的规定

1）《中华人民共和国会计法》

2000年7月修订实施的《中华人民共和国会计法》第四条规定，单位

负责人对本单位的会计工作和会计资料的真实性、完整性负责；第二十七条规定，各单位应当建立、健全本单位内部会计监督制度。

2）《内部会计控制——基本规范》

财政部于2001年颁布实施的《内部会计控制——基本规范》规定，单位负责人对本单位内部会计控制的建立健全及有效实施负责。

3）《企业内部控制基本规范》

财政部于2008年6月28日发布的《企业内部控制基本规范》，要求上市公司自2009年7月1日起施行，鼓励非上市的大中型企业执行。其中第六条规定，企业应当根据有关法律法规、本规范及其配套办法，制定本企业的内部控制制度并组织实施。

4）国资委《中央企业全面风险管理指引》

国资委2006年6月发布的《中央企业全面风险管理指引》第九条规定，企业应本着从实际出发、务求实效的原则，以对重大风险、重大事件（指重大风险发生后的事实）的管理和重要流程的内部控制为重点，积极开展全面风险管理工作。具备条件的企业应全面推进，尽快建立全面风险管理体系；其他企业应制定开展全面风险管理的总体规划，分步实施，可先选择一项或多项业务开展风险管理工作，建立单项或多项内部控制子系统。通过积累经验，培养人才，逐步建立健全全面风险管理体系。

5）香港联交所对内部控制的要求

2004年11月香港联交所发布了《企业管治常规守则》，要求公司董事至少每年审核一次内部控制的有效性，并在《公司治理报告》中向股东汇报。

6）上交所和深交所对内部控制的要求

2006年6月上交所发布《上海证券交易所上市公司内部控制指引》，

2006年9月深交所发布《深圳证券交易所上市公司内部控制指引》，均要求在该证券交易所上市的公司应当按照法律、行政法规、部门规章及本所股票上市规则的规定建立健全内部控制制度，保证内部控制制度的完整性、合理性及实施的有效性，以提高公司经营的效果与效率，增强公司信息披露的可靠性，确保公司行为合法合规。

2. 国外相关法规对上市公司建立内部控制的规定

2002年7月颁布美国《萨班斯法案》第404条款，要求在美上市公司必须建立并保持有效的财务报告内部控制，并要求财务报告的签署人对此负责。

《萨班斯法案》以维护广大投资者利益为宗旨，对惩治公司财务欺诈、规范企业行为和加强资本市场监管做出了规定，其内容主要包括：

① 明确公司管理层的责任。明确公司管理层对披露报告真实、全面、准确负责，公司首席执行官和首席财务官须签字对财务信息的准确性负责。公司必须实时公布任何导致公司财务健康状况发生变化的事件。明确公司管理层对内部控制体系设计、建立、运行有效负责。

② 要求公司的外部审计师对公司与财务报告相关的内部控制的有效性执行审计程序，并出具审计报告。

③ 加强会计监管。《萨班斯法案》一方面加重对公司管理层违规行为的惩罚，另一方面加强对会计行业的监督。美国证券交易委员会设立独立的上市公司会计监管委员会来监督会计行业，该委员会制定了清晰统一的职业标准和道德规范，并具有调查渎职和违规的权力。

④ 完善公司内部审计制度。该法案第301条要求所有的上市公司都必须设立审计委员会，该委员会的成员必须全部是“独立董事”。

⑤ 强化上市公司信息披露的监控。SEC必须在三年期限内对每个上市公司提交的信息披露进行审查，并做出审查结论。

⑥ 突出舞弊防范。法案对欺诈和舞弊防范措施做了强制规定，要求建立“反舞弊程序和控制”并每年进行评估，高层管理人员有任何程度上的舞弊行为就会被认定内部控制无效。

1.3.2 相关人员在内部控制中的责任

1. 管理层的内部控制责任

（1）《萨班斯法案》的要求

根据美国上市公司会计监督委员会（PCAOB）制定的内部控制“审计标准”（Auditing Standard），要求公司管理层对内部控制的有效性实施评估，并且对所实施的评估进行记录和报告。管理层的总体责任包括：

① 管理层必须记录与所有重要财务报表会计科目和披露事项之相关认定有关的内部控制设计。

② 管理层必须测试与所有重要财务报表会计科目和披露事项之相关认定有关的内部控制，而且测试应当涵盖内部控制的全部要素。

③ 管理层必须执行适当程序以获得充分的证据并保留相关记录，从而支持其对于公司内部控制的有效性实施的评估。

④ 管理层对内部控制实施评估是公司内部控制的一部分，它代表了公司监督内部控制的一个重要方面。可以使用内部审计师、公司其他人员和第三方协助其进行评估工作，但不能将其对公司内部控制进行评估的责任委派给外部审计师或其他任何第三方。

⑤ 如果发现了一个或多个重要缺陷（Material Weakness），管理层就不

能认定公司的内部控制是有效的。

⑥ 管理层报告必须披露所有重要缺陷。

（2）《内控规范》的要求

1）董事会

对内部控制的建立健全和有效实施全权负责（《内控规范》第十二条）。

2）监事会

对董事会建立与实施内部控制进行监督（《内控规范》第十二条）。

3）管理层

- 成立专门机构或者指定适当的机构具体负责组织协调内部控制的建立与实施及日常工作（《内控规范》第十二条）。
- 对公司内部控制的有效性进行自我评价，披露年度自我评价报告（《通知》）。
- 不强制要求对内部控制的有效性进行审计（《通知》）。

4）审计委员会

监督内部控制的有效实施和内部控制自我评价情况（《内控规范》第十三条）。

2. 单位负责人的内部控制责任

在有关法规中均明确了单位有关负责人在内部控制的责任，可概括为：

（1）美国《萨班斯法案》对管理层的规定

《萨班斯法案》第302条款和第404条款，分别对单位负责人在财务报告及内部控制中的责任作了规定

① 在302条款中，要求向美国证券交易委员会提交定期财务报告的公司，在每个年度或季度定期报告中就某些财务事宜附一份由公司首席执行

官和首席财务官签署的书面认证文件，以保证公司提交的财务报告在所有重大方面公允地反映了公司的财务状况和经营业绩。

② 在404条款中，在披露年度报告时，首席执行官和首席财务官就内部控制有效性发表声明。

- 《萨班斯法案》针对上市公司增加了许多严厉的法律措施，成为继20世纪30年代美国经济大萧条以来，政府制定的涉及范围最广、处罚措施最严厉的公司法律。
- 董事和高层管理人员须返还因公司虚假报表取得的激励性报酬和买卖股票收益。
- 对于违反财务报表披露要求的行为，个人的处罚额提高到100万美元，并可同时判处的监禁期限延长到10年，对恣意违反财务报表披露要求的公司主管处罚额高达500万美元，并可判处高达20年的监禁。

相关链接

《萨班斯法案》解读

- 《萨班斯法案》第302条款要求公司首席执行官及首席财务官对以下事项做出声明：
  — 他们已复核了财务报告。
  — 报告中不存在任何重大错报和漏报。
  — 报告中的财务报表及其他财务信息在所有重大方面公允地反映了公司的财务状况和经营成果。
  — 对建立和维护内部控制负责。在财务报告提交前的90天内，对内部控制的有效性进行评价，向审计师及审计委员会披露内部控制中存在的重要缺陷及内部控制系统中关键人员的舞弊

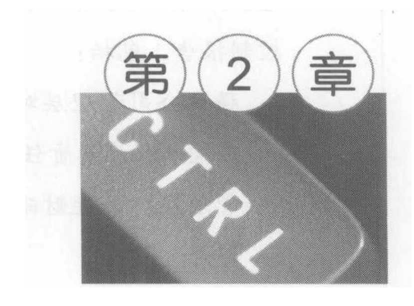
> 行为（如有），评价控制程序后，对内部控制发生的重大变化及管理层采取的更正措施做出陈述。
>
> - 《萨班斯法案》第 404 条款要求公司编制的年度报告中包括内部控制报告，包括：
>   — 强调公司管理层对建立和维护充分有效的内部控制系统及相应控制程序的责任。
>   — 管理层对最近财政年度末内部控制体系及控制程序有效性的评价。
>   — 要求公司的审计师对公司与财务报告相关的内部控制有效性执行审计程序，并出具审计报告。该审计应当遵循 PCAOB 发布或认可的准则。

（2）《内控规范》对管理层的要求

《内控规范》要求管理层对公司内部控制的有效性进行自我评价，披露年度自我评价报告，但不强制要求对内部控制的有效性进行审计。没有规定具体处罚内容的条款。

3．其他员工的内部控制责任

公司的所有员工都必须严格执行内部控制的各项规定，在其责任范围内协助首席执行官和首席财务官设计、建立、记录并维护有效的内部控制。同时，有责任确保提供准确、完整的财务报告信息。此外，及时向管理层汇报所知的任何重大错误、舞弊和/或非常规事项，确保公司内部控制执行有力。



风险评估

2.1 风险概述

2.1.1 风险的概念

所有公司，无论规模、结构和行业性质，都面临着诸多来自内部和外部的风险，影响公司既定目标的实现。例如，公司面临原材料价格上涨的市场风险，产品质量不合格的经营风险，违反法律法规的合规风险等。风险是指未来的不确定性的因素和事项对公司实现目标的影响。

可见，它突出了以下方面：风险是关于“未来的不确定性”，所有的人都不确定将来的事情，因此是将来存在的风险；风险与企业经营目标紧密相关，一般来说，企业目标定得越高风险越大，目标定得越低风险越小。

需要注意的是，风险对实现企业的经营目标有坏处，也可能有好处。所谓好坏或正面负面都是指对结果的判断而言的，风险本身无所谓好坏。把风险看做纯粹的负面的东西，有利于专注防范风险带来负面影响，但同时有可能忽略风险中蕴藏的机会。因此，企业对风险正负面影响的考虑应该结合在一起，这同“没有风险就没有回报，高回报蕴涵着高风险”的观点是一致的，收益是对承担风险的补偿。

相关链接

风险的定义

- 2009 年 11 月 13 日，国际标准化组织颁布了风险管理标准（*ISO 31000：2009 Risk management——Principles and guidelines*），为风险管理提供了原则和通用准则，ISO/IEC Guide 73：2009 也于同期发布，为风险管理提供通用术语定义。其中“风险”的定义是风

> 险管理标准的核心概念，经 ISO 风险管理工作组 4 次会议的激烈讨论，将“风险”定义确定为“不确定性对目标的影响”。
> 来源：*ISO31000：2009 Risk management—Principles and guidelines*

2.1.2 风险的特性

风险具有以下特性：

① 风险具有不确定性。风险什么时间、地点发生是没有规律的。

② 风险具有客观性。风险是客观存在的，只要企业存在该业务，那么相对应的风险就应该存在，而不论在哪级管理层面上，也不会因为企业具有严密的控制措施而消失，也不能因为目前风险没有发生，就判断没有此项风险。

③ 风险具有对应性。风险是与业务相对应的，不同的业务存在不同的风险，不能将甲业务的风险列在乙业务上。

④ 风险具有可避免性。风险是可以认识，并可通过采取控制措施加以规避的。

2.1.3 风险的分类

1. 按风险影响结果划分

风险按其影响结果分为经营决策风险、违反法律法规风险、财务报告失真风险、资产安全受到威胁风险和营私舞弊风险五类。

（1）经营决策风险

经营决策风险是指影响决策的时效、依据和质量的风险等，如

① 预算目标脱离实际。

② 没能以合理的价格取得物资或服务。

③ 投资决策失误导致投资失败。

④ 产品不能及时适应市场的变化和需求。

（2）违反法律法规风险

违反法律法规风险是指没有全面执行国家法律、法规和政策规定的风险，如

① 合同条款违法。

② 偷税。

③ 违反现金管理条例坐支现金。

④ 污染物的排放不符合国家环保规定。

（3）财务报告失真风险

财务报告失真风险是指企业未完全按会计准则、制度等规定组织会计核算和披露信息，导致财务报告在完整性、准确性等方面存在问题，如

① 将资本化的支出费用化或将费用化的支出资本化。

② 会计记录错误（金额、科目、期间错误）。

③ 账实不符。

④ 产品交接计量错误。

（4）资产安全受到威胁风险

资产安全受到威胁风险是指由于管理制度不健全或执行不到位，企业实物资产如设备、存货、证券、资金和其他资产的安全受到威胁，如

① 挪用现金。

② 存货毁损被盗。

③ 资产处置未经适当的授权导致资产流失。

（5）营私舞弊风险

营私舞弊风险是指以故意的行为获得不公平或非法的收益，如

① 人为调节收入。

② 挪用现金。

③ 与审计师合谋篡改审计报告。

④ 偷税。

2．按风险重要程度划分

风险按照其重要程度划分为关键风险和一般风险。

（1）关键风险

关键风险是指影响重大，其发生的频率、后果、影响金额较大的风险。关键风险的发生将直接会导致财务报告的错报，或重大经营损失，或舞弊行为的发生。对于关键风险要给予重点防范。

（2）一般风险

一般风险是指影响不大，其发生的频率、后果、影响金额较小的风险。

风险重要程度的判断主要根据风险发生的可能性和影响程度来确定。

库存现金管理存在的风险如表 2-1 所示。

表 2-1　风险重要程度判断举例——库存现金风险

风　　险	关键风险	可 能 性
出纳岗位未按相关规定进行岗位分离和轮换	√	较大
现金收付未经过适当的授权（包括申请、复核和审批等）		较大
现金收入、支付不符合相关法律法规的规定		较大
库存现金余额账实不符	√	较大

3．按风险应对策略所在层面划分

风险按照其应对策略所在层面的不同，分为公司层面风险和业务层面风险。

（1）公司层面风险

公司层面风险是从公司整体角度对实现战略目标和对公司整体声誉等方面产生负面影响的因素，如宏观经济的不确定性风险、关联交易公平性风险、舞弊风险等。

（2）业务层面风险

业务层面风险是指与公司的主要生产经营活动及管理职能有关的风险，包括采购、生产、市场营销、销售、技术开发，以及研发、人力资源管理、财务管理等业务和管理活动中存在的风险。

4. 按是否为企业带来赢利划分

以能否为企业带来赢利等机会为标志，可以将风险分为纯粹风险（只有带来损失一种可能性）和机会风险（带来损失和赢利的可能性并存）。

相关链接

纯粹风险与机会风险

- 纯粹风险，也叫无意识风险，如欺诈或产品滞销的风险。此类风险只有负面影响，通常是由内部因素导致的，如财务欺诈风险或者由于人力资源部门、运营部门、IT 部门或战略部门的问题而出现的风险。无意识风险构成企业经营的间接成本。
- 机会风险，也叫战略风险，也就是公司为了追寻战略目标而承担的风险，如进入新市场的风险。战略风险既有负面影响，又有正面影响，通常都是由外部因素（如市场、客户、供应商及监管机构等）引起的。企业需要仔细评估这些风险，使之符合自身的战略和风险承受度。

综上所述，风险的分类如图 2-1 所示。

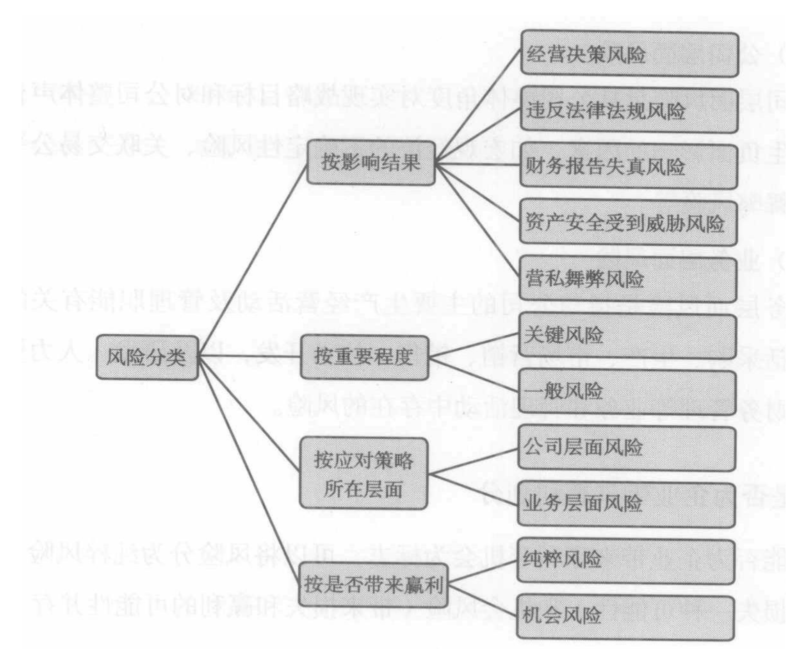


图 2-1　风险的类别

2.1.4　风险承受度

根据《内控规范》第二十一条，风险承受度是企业能够承担的风险限度，包括整体风险承受能力和业务层面的可接受风险水平。

首先，公司需要针对某目标设立一个总体的风险承受度，即确定公司可以承受的目标最大值和目标最小值。

其次，将该目标在多个业务单元（层面）内自上而下进行分解，公司就可确定分解到业务单元（层面）后该目标的风险承受度，即确定各业务单元偏离其目标的最大值和最小值，但业务单元的风险承受度在汇总后不能超出总体的风险承受度。

比如，某公司2010年的销售目标是在2009年的基础上增长20%，达到人民币10亿元，旗下有2个业务单元甲和乙，目标分别是4亿元与6亿元。如果销售目标总体可以承受的目标最小值和目标最大值分别是8亿元和15亿元，然后在甲乙两个业务单元进行分解，甲单元可以承受的目标最小值和目标最大值分别是3亿元和6亿元，乙单元可以承受的目标最小值和目标最大值分别是5亿元和9亿元，如图2-2所示。

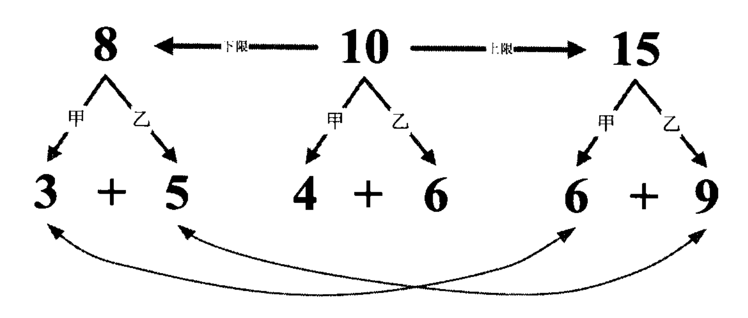


图2-2 风险承受度分解

从图2-2可以看出，该公司2010年针对销售目标总体的风险承受度是8亿～15亿元；业务单元层面，甲单元的风险承受度是3亿～6亿元，乙单元的风险承受度是5亿～9亿元。

根据《内控规范》的要求，确定相应的风险承受度，企业应当准确识别与实现控制目标相关的内部风险和外部风险。

（1）企业识别内部风险，应当关注下列因素

- 董事、监事、经理及其他高级管理人员的职业操守，员工专业胜任能力等人力资源因素。
- 组织机构、经营方式、资产管理、业务流程等管理因素。
- 研究开发技术投入、信息技术运用等自主创新因素。

- 财务状况、经营成果、现金流量等财务因素。
- 营运安全、员工健康、环境保护等安全环保因素。
- 其他有关内部风险因素。

（2）企业识别外部风险，应当关注下列因素

- 经济形势、产业政策、融资环境、市场竞争、资源供给等经济因素。
- 法律法规、监管要求等法律因素。
- 安全稳定、文化传统、社会信用、教育水平、消费者行为等社会因素。
- 技术进步、工艺改进等科学技术因素。
- 自然灾害、环境状况等自然环境因素。
- 其他有关外部风险因素。

相关链接

风险承受度

- 2004 年 COSO《企业风险管理——整合框架》引入了风险容量（Risk Appetite）和风险容限（Risk Tolerances）两个概念。风险容量是指一个企业在追求价值的过程中愿意接受的风险水平，它在战略制定和相关目标选择时起到风向标的作用。风险容限是指对于一项具体管理目标可以接受的偏离程度。
- 《内控规范》第二十一条："企业开展风险评估，应当准确识别与实现控制目标相关的内部风险和外部风险，确定相应的风险承受度。风险承受度是企业能够承担的风险限度，包括整体风险承受能力和业务层面的可接受风险水平。"
- 《内控规范》将风险容量和风险容限统一用风险承受度表示。

2.2 风险评估的一般程序

2.2.1 风险评估的概念

风险评估是企业及时识别、系统分析经营活动中与实现内部控制目标相关的风险，合理确定风险应对策略的过程，是风险管理的基础。在风险评估中，既要识别和分析对实现目标具有阻碍作用的风险，也要发现对实现目标具有积极影响的机遇。

2.2.2 风险评估的一般程序与方法

风险评估主要经过目标设定、风险识别、风险分析、风险应对四个基本程序，如图 2-3 所示。

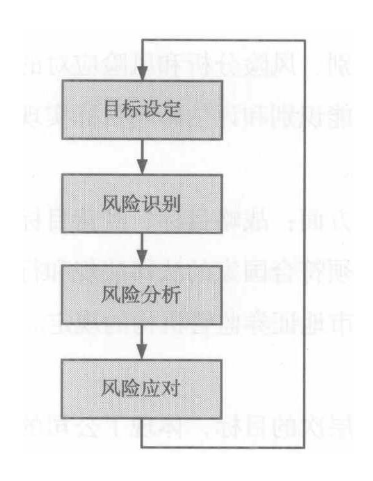


图 2-3 风险评估的一般程序

相关链接

风险识别模型

- 风险识别模型可以分为四类：一是目标导向型风险识别，任何可能危及整体及部分目标实现的事件都可以视做风险；二是情景导向风险识别，情景可以理解为达到目的的不同方式，任何触发不希望情景的事件都被视做风险；三是分类导向风险识别，依据风险事故对风险实施编辑；四是经验导向风险识别，将经验转化为知识库，如对常见风险做出检查表，进行对照等。
- 《内控规范》中的风险评估属于典型的目标导向分类风险识别，认为风险评估由企业战略目标指引和决定，对企业战略目标的确定与认同是开展风险评估的基础工作。因此，风险评估的首要步骤是目标设定，目标设定首要是战略目标。

1．目标设定

目标设定是风险识别、风险分析和风险应对的前提。公司必须首先制定目标，在此之后，才能识别和评估影响目标实现的风险并采取必要的行动对这些风险实施控制。

公司目标包括四个方面：战略目标、经营目标、合规性目标和财务报告目标。目标的确定必须符合国家的法律法规和行业发展规划，符合公司战略发展计划，符合上市地证券监管机构的规定。

（1）战略目标

战略目标是公司高层次的目标，体现了公司的长远发展目标和方向。广义上讲还包括公司的愿景、使命。

以华为公司为例：

愿景 丰富人们的沟通和生活。

使命 聚焦客户关注的挑战和压力，提供有竞争力的通信解决方案和服务，持续为客户创造最大价值。

以客户为中心的战略 为客户服务是华为存在的唯一理由；客户需求是华为发展的原动力。质量好，服务好，运作成本低，优先满足客户需求，提升客户竞争力和赢利能力。持续管理变革，实现高效的流程化运作，确保端到端的优质交付。与友商共同发展，既是竞争对手，也是合作伙伴，共同创造良好的生存空间，共享价值链的利益。

（2）经营目标

经营目标是关于公司经营的效果和效率，包括业绩和利润性目标，以及公司生产经营持续进行的资源保障等。制定符合实际的经营目标是保证战略目标实现的要求，如年度销售目标、新产品开发计划、利润目标等。同时，公司也应考虑经营目标是否会对财务报告产生影响，并予以重点关注。

（3）报告目标

报告目标是关于编制可靠的报告，包括内部和外部报告目标，可能涉及财务和非财务信息。比如，为公司管理层提供准确、完整的经营管理信息，为对外披露提供真实、准确、完整、及时的财务会计报告及其相关资料。

（4）合规性目标

公司必须遵守中国法律法规、海外企业当地法律法规和上市地法律监管规定，而且采取必要的具体行动。各种适用的法律法规确立了公司融入其合规性目标的最低的行为准则。

目标类别及关系如图 2-4 所示。

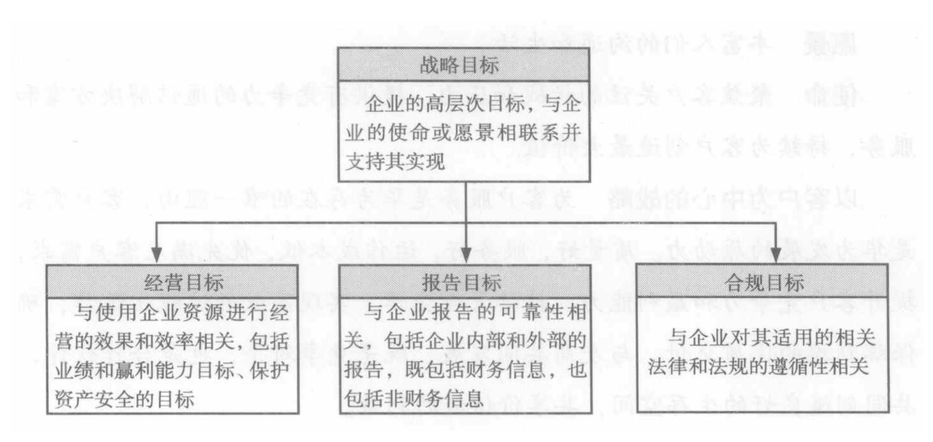


图 2-4　目标类别及关系

2．风险识别

风险识别是指查找公司各项重要经营管理活动及其重要业务流程中存在的影响目标实现的风险和机遇的过程。

（1）风险识别的主要方法

风险识别的主要方法如图 2-5 所示。

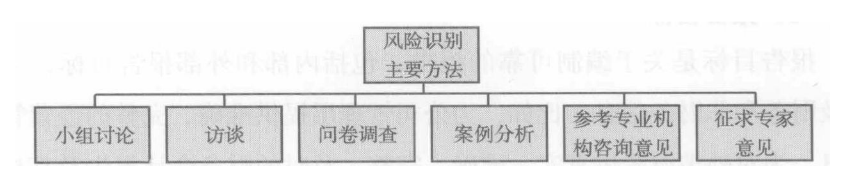


图 2-5　风险识别的主要方法

① 小组讨论。内部控制管理部门组织风险管理人员和相关部门具有丰富经验的管理人员，按业务类别和人员构成进行分组讨论，形成意见。

② 访谈。内部控制管理部门组织人员，制定详细的访谈计划，对相关部门熟悉业务流程的管理人员进行访谈，了解和讨论存在的风险，形成访谈记录。

③ 问卷调查。内部控制管理部门编制风险调查问卷，收集、整理反馈意见确定相关风险。

④ 案例分析。内部控制管理部门定期收集公司或同行业发生的有关案例，组织相关人员进行讨论，通过对案例中妨碍目标实现的负面因素进行分析来识别风险。

⑤ 参考专业机构咨询意见。内部控制管理部门通过向专业机构（如风险管理咨询公司、公司法律顾问等）进行咨询，参考专业机构提供的风险数据库或咨询意见，结合公司实际情况识别风险。

⑥ 征求专家意见。对初步识别形成的风险数据库，内部控制管理部门通过召开座谈会、评审会等形式，向公司内、外部有关专家、学者征求意见。

（2）公司风险识别的概述

风险识别应分别从公司层面、业务层面，动态识别影响公司战略目标及相关目标实现的、内部和外部的各种不确定性因素。

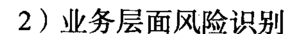
1）公司层面风险识别

从公司战略发展的角度，识别影响目标实现的因素，识别公司层面面临的所有重大的不利因素和有利因素，从而识别风险，发现机遇。这些因素来自外部和内部两个方面：外部因素主要包括政治因素、经济因素、社会因素、自然环境因素等；内部因素主要包括基础设施因素、员工因素、流程因素和技术因素等。

收集、分析、整理对公司内部、国内同行业和国外同行业的风险事件及案例，初步形成风险数据库；通过分析历史数据和行业资料，查找风险发生的内外部原因，分析风险发生的可能性和影响程度，运用公司的风险评估标准对风险评分，确定公司层面重大风险清单。举例如表 2-2 所示。

表 2-2 公司层面重大风险清单举例

序号	风险名称	风险类别	风险描述			涉及的重要业务	涉及的重要部门或企业
			风险说明	损失或影响	风险原因		
1	资金流风险	经营风险	资金流动性风险是指由于销售萎缩、货款回收不及时、企业税负较重、运营成本上升、融资渠道不畅等原因，导致资金不足，影响企业运营和投资目标的实现	企业没有充足的资金，可能造成企业日常生产经营活动中断、承诺的投资项目无法实施，从而阻碍企业可持续经营目标或企业成长目标的达成，并且使投资者对企业持续运营能力的信心受挫	① 国际金融危机严重冲击全球经济，出口持续低迷，我国经济下行压力加大，市场需求萎缩，直接影响公司的收入和效益 ② 公司的投资总量稳定增长，税收及成本支出呈上升趋势	资金、销售、投资、研发、生产等	财务部门、销售部门
2	健康安全环境风险	经营风险	健康安全环境风险是指公司业务活动中可能造成的职业病、人员伤亡、资源浪费和生态环境破坏的风险	可能导致索赔、罚款；可能导致生产经营业务中断或终止；可能引起社会的广泛关注，给企业声誉造成负面影响	① 工作场所或生产经营过程具有易燃易爆、高温高压、有毒有害等特点 ② 人员流动性加大，员工基本素质低，知识和能力培养难度大，接受培训不足 ③ 违反操作规程和劳动纪律 ④ 作业情况复杂，技术要求高，存在不稳定性	生产、人力资源、技术等	公司的所有部门及下属企业
3	……		……	……	……	……	……



2）业务层面风险识别

业务层面风险识别是通过根据一定的规范、采用一定的方法对业务流程进行描述，在业务流程描述的基础上，以业务流程步骤为主线，全面识别影响目标实现的相关因素。

业务层面风险评估从财务报告目标出发，具体参考本书第 3 章介绍的方法，确定财务报表中的重要会计科目和重要业务流程，按照风险评估的基本程序对会计科目的存在与发生、完整性、估价与分摊、权利与义务、表达与披露的风险进行评估，初步建立了财务报告风险数据库。举例如表 2-3 所示。

表 2-3　报告风险数据库举例

流　程	子 流 程	相关风险
财务报告	会计业务外理	会计业务处理缺乏适当的权责分离
		账账、账实不符，会计信息不准确
		会计记录处理未经有效授权（ERP）
		未及时发现或处理接口传递中的错误数据（ERP）
	减值准备	坏账准备的计提和转回不及时、不准确
		坏账准备的计提和转回未经有效审批
		坏账准备的会计估计不合理，坏账准备计算不准确
		账龄的统计和记录不准确
		存货跌价准备的计提和转回不及时、不准确
		存货跌价准备的计提和转回未经有效审批
采购	生产采购	对供应商数据库更新不及时或修改错误
		未经授权修改供应商的信息
		物资采购处理缺乏适当的权责分离
		应当支付的金额不准确
		预付款项与合同规定不符
		暂估存货入库记录不准确、不完整
		重复付款
……	……	……

在公司业务流程梳理的同时，逐步开展业务活动层面经营风险、合规风险的评估工作，逐步形成业务活动层面经营风险数据库。举例如表 2-4 所示。

表 2-4　经营风险数据库举例

风险类	风险定义	风险描述
投资风险	由于缺乏对新建项目的专业评估和有效审批等因素，导致投资决策失误或投资项目回报率低	新建项目选择不符合公司经营目标及需要
	由于年底投资计划未经有效审批、未完全按照计划下达内容组织有效实施等因素，造成计划外项目，影响投资目标的实现	年度投资计划的执行与计划不符
公共关系风险	公共关系风险是指因路演管理、危机管理、媒体监测等口径不一致、职责不明确、归口部门职责缺乏，可能导致公共关系工作不适当而损害公司公众形象的风险	① 未能满足境内外监管机构及投资者咨询问题的要求 ② 路演报告及问答提纲内容不真实、不准确、不完善 ③ 突发事件发布的内容不真实、不准确 ④ 发布信息内容不真实、不准备、不完整 ⑤ 媒体应答信息内容不真实、不准确
信用风险	信用风险是指由于交易对手不执行履约责任而导致的风险。主要表现在交易对手违约、单一客户信用集中度风险、合约对手清偿能力和清偿意愿的不确定性带来的信用风险等	① 对各对家浮动盈亏及超限情况掌握不及时、不准确 ② 未经授权或审批授予对家信用额度 ③ 记录各对家的盈亏数据不准确
……	……	……

3. 风险分析

风险分析主要从风险发生的可能性和对公司目标的影响程度两个角度来分析。在风险分析的过程中，设定一个统一的标准对各个风险发生的可能性和影响程度分别进行定量的评分，从而按风险值（=风险可能性分值×风险影响分值）对风险进行排序。

一般来说，风险发生的可能性可分为基本确定、极可能、可能、可能性低和可能性极低五类，风险造成的影响程度可以分为灾难、重大、中等、轻微、可以忽略五类；为了量化表示，可以将这五类分别以 5、4、3、2、1 五个数字进行评分。

风险分析方法一般采用定性和定量方法组合而成。在风险分析不适宜采取定量分析的情况下，或者用于定量分析所需的足够可信的数据无法获得，或者获取成本很高时，公司通常使用定性分析法。

（1）风险发生的可能性分析（频率、概率）

可能性分析是指假定不采取任何措施去影响经营管理进程的情况下，将会发生风险的概率大小的分析。

由于不同类别的风险，很难用一个统一的、固定的概率或次数来划分，因此，可以按不同的风险类别设定不同的划分标准来确定风险可能性级别。风险可能性的级别确定，可以采用风险发生的概率或一定时期风险发生的次数来判断。

① 比如，如果能够判断相关风险发生的概率，我们可以采用下面的标准：

- 如果风险发生的概率大于 0 但小于或等于 5%，我们确定为风险“可能性极低”。
- 如果风险发生的概率大于 5%但小于或等于 35%，我们确定为风险

"可能性低"。

- 如果风险发生的概率大于 35%但小于或等于 50%，我们确定为风险"可能"。
- 如果风险发生的概率大于 50%但小于或等于 95%，我们确定为风险"极可能"。
- 如果风险发生的概率大于 95%但小于 100%，我们确定为风险"基本确定"。

这种标准适用于可以通过历史数据计算出风险发生概率的风险，如某个地区人均寿命。

② 比如，如果能够判断一定时期风险发生的次数，我们可以采用下面的标准：

- 今后 10 年内发生的可能少于 1 次，我们确定为风险"可能性极低"。
- 今后 5 ~ 10 年内可能发生 1 次，我们确定为风险"可能性低"。
- 今后 2 ~ 5 年内可能发生 1 次，我们确定为风险"可能"。
- 今后 1 年内可能发生 1 次，我们确定为风险"极可能"。
- 今后 1 年内至少发生 1 次，我们确定为风险"基本确定"。

这种标准适用于大型自然灾害/不可抗力因素的潜在风险，如地震、海啸、政治动乱等。

上述两个标准如表 2-5 所示。

表 2-5　可能性评估标准

评分	可能性（定性）	发生概率（定量）	一定时期风险发生的次数（定量）
5	基本确定	≥95%	今后 1 年内至少发生 1 次
4	极可能	50% ~ 95%	今后 1 年内可能发生 1 次
3	可能	35% ~ 50%	今后 2 ~ 5 年内可能发生 1 次
2	可能性低	5% ~ 35%	今后 5 ~ 10 年内可能发生 1 次
1	可能性极低	<5%	今后 10 年内发生的可能少于 1 次

对于风险发生的概率的估计，一般考虑以下因素：

一是与风险相关的资产的变现能力（主要指变现难易程度）。如果资产变现能力越强，则风险发生的概率就高；反之，风险发生的概率就低。

二是经营管理中人工参与的程度。凡是人工参与程度越高，而自动化程度越低，则风险发生的概率就越高；反之，风险发生的概率就低。

三是经营管理中是否涉及大量的、繁杂的人工计算。凡是涉及大量的、繁杂的人工计算，风险发生的概率就高；反之，风险发生的概率就低。

四是要参考相关风险事件过去发生的情况。如果曾经发生过，而且带有普遍性，那么风险发生的概率就高；反之，风险发生的概率就低。

五是要预计公司未来发展及业务变化情况。如果公司高速发展，而且业务复杂、变化频繁的话，风险发生的概率就高；反之，风险发生的概率就低。

（2）风险影响程度分析

风险分析中，除了进行风险发生可能性分析外，还要对风险影响程度进行分析。风险影响程度分析主要指风险对目标实现的负面影响程度，风险造成的影响程度可以分为灾难、重大、中等、轻微、可以忽略五类。当然，风险影响程度是相对某个既定目标而言的，所以在进行影响程度分析前，必须明确风险分析相对应的目标是什么，可能存在对经营目标没有影响或影响很小，但对于报告目标影响程度就大的情况。

1）定量分析

定量分析要参考风险承受度，如影响程度超过某个风险对应目标的风险承受度，那么影响程度定位重大及以上；反之，影响程度是中等及以下。表2-6是影响程度定量分析的一个例子。

表 2-6　影响程度定量分析举例

评　分	影响程度	定量分析
5	灾难	影响税前利润达 20%
4	重大	影响 5%～10%的税前利润
3	中等	影响 1%～5%的税前利润
2	轻微	影响小于 1%的税前利润
1	可以忽略	影响小于 1‰的税前利润

定量分析能带来更高的精确度。定量分析一般需要更高程度的努力和严密性，有时采用数学模型。定量分析高度依赖于支持性数据和假设的质量，并且与有着已知历史和做可靠预测的风险暴露高度相关。

2）定性分析

除运用定量分析外，在不适宜采取定量分析的情况下，或者用于定量分析所需的足够可信的数据无法获得，或者获取成本很高时，公司通常使用定性分析法。

如果风险对于目标的实现，将会产生直接的、决定性的影响，就属于风险影响程度“大”，如财务会计报告未经过有效的审核，将会对报告的真实性和准确性产生直接的、决定性的影响，因此，该项风险被认定为影响程度“大”；反之，如果风险对于目标的实现，只是产生间接、非决定性的影响，就属于风险影响程度“小”，如没有定期维修机器设备，对于财务会计报告的真实性、准确性只会产生间接的、非决定性的影响，因此，该项风险属于影响程度“小”。

又如，公司声誉风险很难量化，可以采用定性分析，如表 2-7 所示。

表 2-7　声誉风险定性分析

评　分	影响程度	定性分析
5	灾难	负面消息流传世界各地，被中央政府部门或监管机构高度关注，或开展调查，引起公众媒体极大关注并呼吁采取行动，对企业声誉造成无法弥补的损害

续表

评　分	影响程度	定性分析
4	重大	负面消息在全国各地流传，对企业声誉造成重大损害，被全国性媒体持续报道，被中央政府部门关注
3	中等	负面消息在全国流传，被地方政府部门关注
2	轻微	媒体关注，负面消息在当地局部流传，对企业声誉造成轻微损害
1	可以忽略	负面消息在企业内部流传，企业声誉没有受损

3）定量与定性相结合

很多情况下，因为业务及其风险的自然属性，很难单独定量分析或者定性分析，需要定量分析与定性分析结合起来。比如，表 2-8 所示的环保风险。

表 2-8　环保风险定量与定性结合分析

评　分	影响程度	定量与定性结合分析
5	灾难	无法弥补的灾难性环境损害；需要 3 年以上的时间来恢复，或者人类所掌握的现代科技尚无法恢复激起公众的愤怒和口诛笔伐；潜在的大规模的集体诉讼的迹象
4	重大	造成主要的、长期的环境损害；需执行重大的补救措施，且要 6 个月到 3 年左右的时间来恢复；大规模的公众投诉
3	中等	对环境造成中等影响；需一定程度的补救措施，需 6 个月或以内的时间才能恢复；出现个别投诉事件
2	轻微	对环境或社会造成一定的影响，但不破坏生态系统；被政府有关部门关注或需要通知政府有关部门可不采取行动
1	可以忽略	对环境或社会造成短暂的影响，可不采取行动

相关链接

风险分析的方法

- 当代企业应用最为广泛的几种风险度量与分析方法包括：风险价值法（Value at Risk，VAR）；情景分析法；风险调整资本收益法

（Risk Adjusted Return on Capital，RAROC）；经济资本法。

- 国资委《中央企业全面风险管理》附录“风险管理常用技术方法简介”介绍了以下几种方法：风险坐标图、蒙特卡罗方法、关键风险指标管理和压力测试等。
- 企业根据自身实际选取适合自己的方法，确定恰当的标准来分析风险。例如，前几年石油企业发生井漏事故，该风险对于安全、环境、企业声誉、财务、法律等方面都有一定的影响，这就需要从中选择一个影响最为严重的方面，如安全标准。

（3）风险重要性水平的判断（确定关键风险）

按风险值（=风险可能性分值×风险影响分值）对所识别的风险进行排序，得到公司风险划分为高、中、低、较低四个风险领域，用风险热力图表示。图 2-6 是一个风险热力图的例子，也叫风险地图，或风险共同语言。

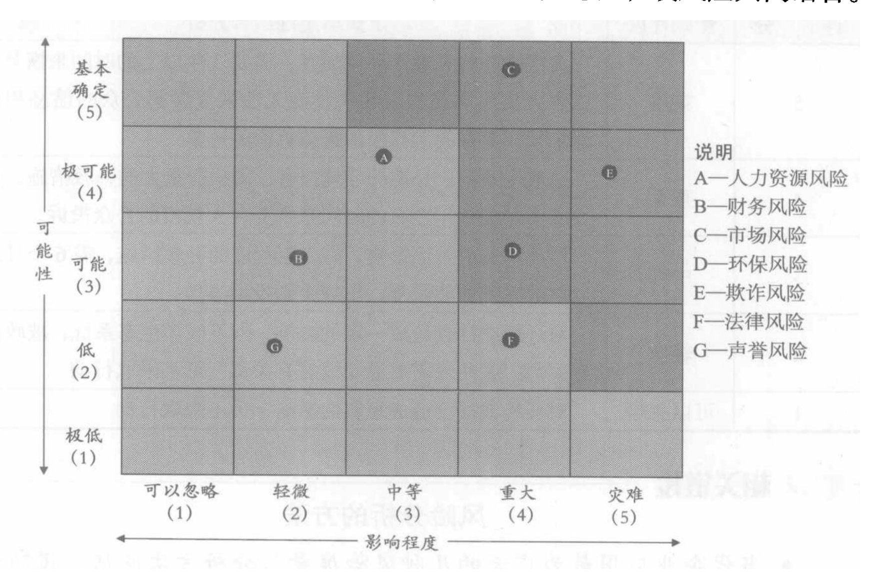


图 2-6　风险热力图

根据图 2-6 所示的风险热力图，确定风险的重要性水平，以决定投入的关注程度或实施风险应对的力度和时间。对于重要性水平为低和较低的风险，由于其发生的可能性和影响程度均较小，如财务风险（B）和声誉风险（G），公司可以忽略此类风险而不予关注。对于重要性水平为中的风险，如人力资源风险（A）和法律风险（F），公司将此类风险确定为一般风险并给予一般关注。对于重要性水平为高的风险，公司将此类风险确定为关键风险并给予重点关注，如市场风险（C）、环保风险（D）和欺诈风险（E）就是关键风险。一般风险和关键风险的划分是公司确定风险应对策略和制定控制措施的一个重要依据。

4. 风险应对

（1）风险应对方案

风险应对是指选择和运用具体管理措施对风险进行管理的过程，主要是在风险识别和风险分析完成后，公司确定如何应对风险，并将方案付诸实施。风险应对的目的是将剩余风险控制在风险承受度以内。风险管理的最终目的是利用公司现有的资源对公司所面临的风险，分不同情况采取管理措施进行应对。

风险应对策略一般包括风险规避、风险降低、风险分担和风险承受四种，表 2-9 是对四种风险应对策略的分析。

表 2-9 风险应对方案分析

序号	应对类型	含 义	适应特征	方法举例
1	风险规避	放弃或者停止与该风险相关的业务活动	该风险超出风险承受度；与企业战略关联度较小；风险回报率不佳；企业现有条件下还没有能力控制该方面的风险	放弃或不接受暗含该风险的新机会；停止某业务，放弃与退出市场；抛售（个别或某些）业务；禁止（限制）某些高风险活动（通过政策、处罚、设防等方式）

续表

序号	应对类型	含　义	适应特征	方法举例
2	风险降低	采取适当的控制措施降低风险或者减轻损失	为实现企业战略而不可摆脱的固有风险；对风险的损失已经有所准备。"控制"为减少风险的主基调	风险分散管理原则（如分散资产的类别）；隔离控制原则；全方位管理控制；实施特定风险的特定控制程度；预算出可能的损失额度，计划好自筹资金的对冲方式；制定风险应对计划
3	风险分担	借助他人力量，采取业务分包、购买保险等方式和适当的控制措施	风险发生频率不高，但可能损失太大；市场上已经存在较好的风险转移工具	保险合约（通用合约，量身度造合约）转移；衍生金融工具转移；保险——资本市场混合新工具转移）；通过联盟签约等联合承担风险，实现部分风险转移；其他签订合约的专业方法
4	风险承受	不采取控制措施降低风险或者减轻损失	在风险承受度之内；为实现战略而不可摆脱的固有风险；风险稳定，不会再加大；对承受风险损失已经有所准备	预算出可能的损失额度，用额外预留资金或其他风险融资方式对冲；集团内调拨资金平衡总风险；必须制定风险应对计划

（2）确定风险应对方案考虑的主要因素

① 风险应对方案是否符合成本效益原则。风险规避与成本支出相比较。

② 风险应对方案中可能的机遇与相关风险的比较。机遇的收益与风险的损失相比较。

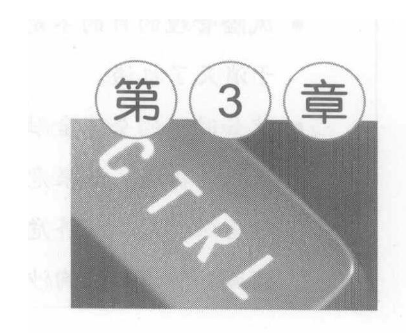
③ 考虑多种风险应对方案的组合。从比较高的层面与高度，以及整个企业的角度去分析风险，考虑风险组合应对，发挥协同效应。

④ 慎重考虑那些发生可能性较小但却很严重的风险，如中国 5·12 地震。

相关链接

风险与机遇

- 风险管理的目的不是消灭风险，而是管理风险，消灭风险也就等于消灭了机遇。
- 就如时下的全球金融危机，“危”虽然意味着危险，但是“机”却意味着机遇。如果危机是百年一遇，那么机遇也是百年一遇。纵观全球，每次经济危机之后，都会造就新的高速增长和新的技术领域。所谓大浪淘沙，凤凰涅槃。



合 规 范 围

做事情，先要确定做什么。范围界定是《内控规范》合规项目的最重要环节之一。在此环节里，必须明确重要会计科目、披露事项，业务流程和子流程及其使用关键信息系统，以及应该纳入范围的组织单位。

财政部企业内部控制标准委员会《企业内控规范起草说明》认为，根据多数企业的意见，借鉴国际有关做法，提出对有义务对外提供财务报告的企业（上市公司），至少须确保财务报告的真实可靠，并着重就影响财务报告真实可靠的重要业务与事项进行了规范，引导企业建立健全以财务报告内部控制为核心的内部控制机制。基于以下考虑：

第一，企业的经营管理活动，归根结底要通过财务报告来反映，抓住了财务报告内部控制这条主线，在一定程度上也抓住了企业经营管理与内部控制的重心和主体。

第二，保证财务报告真实可靠，是企业的法定责任，是维护社会公众利益的基础环节，强化财务报告内部控制机制建设，是提升企业市场形象与诚信度、维护社会公众利益的基本要求。

第三，从政府监管和资本市场监管的角度看，即使是当今世界最发达的国家，也将财务报告内部控制作为企业管理层内部控制自我评估和注册会计师评价的主体，因为满足了财务报告内部控制的要求，能够合理保证企业财务会计信息披露的真实公允，能够有效维护社会公众利益、促进资本市场健康稳定发展。

据了解，将取代《企业内部控制鉴证指引》的《企业内部控制审计指引》（参考附录 B）将明确企业内部控制审计的范围，该指引第二条规定“本指引中内部控制审计的范围，主要是企业为了合理保证财务报告及相关信息真实完整、资产安全而设计和执行的内部控制。用以合理保证资产安全的内部控制，可能涉及合理保证经营效率和效果、经营管理合法合规的内

部控制。”

基于实践及实际操作性，实际上就是与财务报告相关的内部控制，当然这其中肯定会与其他几大目标产生交叉。

3.1 自上而下基于风险的方法

证券分析师经常使用一种称为“自上而下”（Top down）的模式来分析所追踪的股票：从评估整体经济入手，然后对对象公司所处行业情况进行分析，最后切入企业分析；而企业分析，除了最常见的财务数据分析，还涵盖了对公司战略、企业生命周期、产品与市场、营销策略、销售渠道、主要客户、上游供应商与原料、竞争环境等的研究。

案　例

自上而下的风险导向方法

- Rubbermaid 曾是美国全球领先的塑料制品生产商，产品包括储藏罐和垃圾箱等。在 20 世纪 90 年代中期，该公司连续数年的年均增长率超过 14%，且连续三年被《财富》杂志评选为“美国最受欢迎的企业”。
- 对 Rubbermaid 进行战略分析后发现，该公司对原油价格的波动非常敏感，因为塑料制品的一个重要原料是树脂，而树脂是通过原油炼制的。但 Rubbermaid 没有采取任何控制原材料风险的措施：既没有集中采购，也没有与供应商签订长期购买合同。而实际上，该公司是世界上最大的树脂消费商之一，以其采购规模，完全可以通过谈判获得很优惠的价格。但该公司没有利用集中采购所能赋予它的定价能力，而是在全球 12 个地方分别采购。当原油价格上涨时，它只

能把增加的成本转嫁给客户。

- 该公司也未能有效管理与最大客户沃尔玛的关系。沃尔玛拒绝接受价格上涨，并把 Rubbermaid 的产品放在靠里的货架上，而将 Rubbermaid 的低价竞争对手 Sterlite 的产品置于位置最好的货架上。
- 该公司另一个战略方面的问题是制定的增长目标太高，试图维持14%的年增长率。实现目标的困难给管理层形成巨大压力，而这一点对于内部控制环境十分不利。同时，它在欧洲的扩张也遭遇挫折。
- 基于上述情况，我们可做出合理的财务业绩预期：销售增长放缓、销售毛利收窄、利润降低、研发费用需要增加等。假如出现与预期不一致的情形，如这一年的销售毛利反而比去年增加等，我们就要打个问号。同时，我们估计它会通过降低产品质量来降低成本，以达到业绩目标，这就需要对成本结构进行分析，看它有没有改变产品配方来压缩成本；如果它产量过大而销售又不利，它的库存应该会增加；还有资本结构方面，它在欧洲投资失败，这些资本是否作为坏账冲销掉……通过这样一步步的分析评估，可以判断出该公司风险较高的领域。
- 自上而下风险导向方法就是分析研究企业在哪些方面的风险没有防范控制好，它对企业财务报表可能有什么样的影响，然后再通过相互印证的证据来判断报表是否是真实和恰当的。

采用自上而下风险导向方法，将风险评估与范围界定结合起来，确定《内控规范》实施范围，是为最有效率的方法，如图 3-1 所示。

公司目标及风险评估请参考本书第 2 章。公司层面控制（Entity Level Control，ELC）、IT 一般控制（IT General Control，ITGC）和 IT 应用控制（IT Application Control，ITAC）将在后面的章节详细说明。

公司目标

风险评估（第 2 章）

公司层面控制（第 4 章）

IT 一般控制（第 4 章）

合并财务报告

确定合并财务报表层次和科目层次的重要性水平，识别重要会计科目和披露事项

重要会计科目/披露与业务流程对应确定重要业务流程

重要会计科目/披露与关键信息系统对应确定关键信息系统（ITAC）

销售　采购　资金　资产　财务报告

ERP（SAP）　客户关系管理（CRM）　办公自动化（OA）　网络报销　供应链管理（SCM）

业务流程与组织单位对应确定重要组织单位

业务流程目标

信息处理目标

组织单位 A　组织单位 B　组织单位 C

财务报表认定

控制

风险控制矩阵

① 根据业务和信息处理目标，识别风险，评估控制

② 评估控制是否达到财务报表认定要求

图 3-1　基于财务报告的自上而下风险导向方法

本章概括了管理层确定重要会计科目、披露事项、业务流程和关键信息系统及应评估的组织单位的方法。对上述事项的界定与《内控规范》的5个组成要素是相关联的，这5个组成要素是：控制环境、风险评估、控制活动、信息与沟通、监控。

3.2 范围界定的步骤

3.2.1 确定合并财务报表层次和科目层次的重要性水平，识别重要会计科目和披露事项

重要会计科目和披露事项从两个层面予以确定：一是合并财务报表层面；二是单个会计科目或披露事项层面（如存货可以包括产成品、在产品和原材料，收入可以包括产品收入和服务收入）。

1．重要性水平定义

所谓重要性是指一项漏报或误报的金额（单个项目或多项累计），在其所处环境的影响下，使得一个依赖该会计报表的理性人员的判断会因该漏报或误报改变或受到影响。

“重要”一词不仅局限于定量的重要性。某些科目可能从定性的角度或因被投资者视为重要的业绩衡量指标而被看做重要的会计科目。

2．重要性水平的分类

（1）定量标准

分为财务报表层次及会计科目层次的重要性水平。一般以税前利润的5%作为报表层次的重要性水平，会计科目超过报表层次重要性水平的50%

（即税前利润的 2.5%），一般情况下视为重要会计科目。

（2）定性标准

在确认重要会计科目时，先按定量标准进行确认，凡是会计科目的当期余额或发生额大于或等于定量标准的，直接确认为重要的会计科目，对于其他的会计科目，我们还必须从定性的角度，确认是否属于重要会计科目。通常考虑的定性因素包括：

① 科目由复杂的成分组成。例如，收入项目包含多个会计科目或明细科目，它们产生于各种不同的交易类别，如产品收入和服务收入等，因此将收入项目确认为重要的会计科目。

② 会计科目核算的业务存在较大的错误和舞弊的可能性。例如，现金科目的期末余额一般不大，不会超过上述定量标准，但由于现金存在收支发生错误、被盗或舞弊的可能性，管理风险较大，因此从定性的角度将现金科目确认为重要会计科目。

③ 会计科目核算的业务包含的交易数量、复杂程度和类似程度。例如，销售过程中的产品入库、出库，由于频繁发生，发生错误的可能性比较大，因此将存货项目所包含的会计科目确认为重要的会计科目。

④ 会计科目相关的交易事项本身具有较强的经营风险，可能存在重大的财产损失。例如，短期投资存在因为决策失误、证券市场波动而产生重大损失的可能性，因此将短期投资确认为重要会计科目。

⑤ 会计科目核算的内容存在较强的会计估计和人为判断，会计科目确认记录金额具有一定的不确定性，将此类会计科目确认为重要的会计科目。例如，预提费用核算的内容包括预提的利息、尚未支付的保险费及其他的生产经营费用，预提的金额需要一定的估计和判断，存在预提金额不准确的可能性，因此将预提费用确认为重要会计科目。

⑥ 存在潜在的损失和支付风险（如与或有负债相关的会计科目）。例如，诉讼损失、未了结重大事故所产生的预计负债，记录金额需要较强的专业判断和会计估计，并且存在潜在的损失风险和支付风险，因此将此类项目确认为重要的会计科目。

⑦ 相关账务处理的确认、金额计算较复杂。例如，各项减值准备的测算，需要较强的专业判断，并具有较高的专业测算水平，因此将各项减值准备作为重要会计科目。

⑧ 本年度新发生的交易或行为所对应的会计科目。例如，当年新发生的筹建期间的开办费、租入的固定资产改良工程支出，以及摊销期限在一年以上的固定资产修理支出，相对应的会计科目递延资产应确认为重要的会计科目。

⑨ 会计科目核算内容是否包含大量的关联交易。例如，销售存在着大量的关联交易，因此收入确认为重要会计科目。

（3）附属科目的重要性水平

如果根据上述定量和定性的因素确认某项会计科目是重要的，那么其附属科目也是重要的。

例如，固定资产是重要会计科目，其附属的累计折旧、固定资产减值准备等也应确认为重要会计科目。

（4）重要披露事项的确认

财务报告中的每项附注都是报告使用者关心的事项，所以将财务报告的会计报表附注，全部确认为重要的披露事项。在确定重要披露事项时，应将每项附注作为一个整体确认为重要披露事项，而不是针对附注中的个别披露事项。

3.2.2 确定重要业务流程及关键信息系统

重要业务流程是指影响到重要会计科目的业务流程，即与重要会计科目直接相关的流程。关键信息系统是指影响到重要会计科目的信息系统，即与重要会计科目直接相关的流程。将上一步识别的重要会计科目/披露和生成这些重要会计科目/披露的业务流程和关键信息系统联系起来，进行配对，如表 3-1 和表 3-2 所示。

表 3-1 重要会计科目/披露与业务流程对应

重要会计科目\流程	销 售	采 购	资 金	财务报告
流动资产				
货币资金	√	√	√	√
应收账款	√			√
其他应收款	√			√
预付账款		√		√

表 3-2 重要会计科目/披露与关键信息系统对应

流程\系统名称	ERP（SAP）	客户关系管理系统（CRM）	办公自动化系统（OA）	网络报销系统	供应链管理系统（SCM）
关键系统（Y/N）	Y	Y	Y	N	Y
销售	√	√			
采购	√		√		√
财务报告	√				

这有助于确保所有重要的会计科目/披露都能与业务流程对应，以及确保所有的重要业务流程和关键信息系统均被识别。流程根据公司业务流程实际，同时可以参考财政部《企业内部控制应用指引》确定。

重要的业务流程/循环及业务子流程根据机构的不同也有所区分。比如，研发或广告宣传费对于一家消费者产品生产公司来说是一笔巨大的开

支，但对于一家金融服务公司就不会了。

3.2.3 确定重要组织单位

如果业务流程和子流程在多家组织单位进行（如控股公司、不同地域的下属公司），应该确定哪些组织单位纳入范围呢？应考虑下列几大要素：

- 组织单位的相关财务状况和经营状况。
- 组织单位出现重大错报的风险。
- 选定的组织单位的业务流程和内部控制程序在集中处理或共享服务环境中所占的比例。

重要组织单位是指在数量或性质上达到一定标准，需要纳入《内控规范》合规范围的组织机构或业务单位。确定重要组织单位的步骤如图 3-2 所示。

1. 定量标准

如果至少满足下列合并财务报表指标之一的组织单位，纳入《内控规范》合规范围：

- 大于年度收入的 5%。
- 大于税前利润的 5%。
- 大于总资产的 5%。
- 大于所有者权益的 5%（如可行）。

这些指标可根据具体的组织结构做相应调整。比如，如果一家公司采用集中化的经营模式，拥有多家规模类似的业务单位，那么这家公司可用来确定本身重要的组织单位的比例则应降低至 1%或 2%。

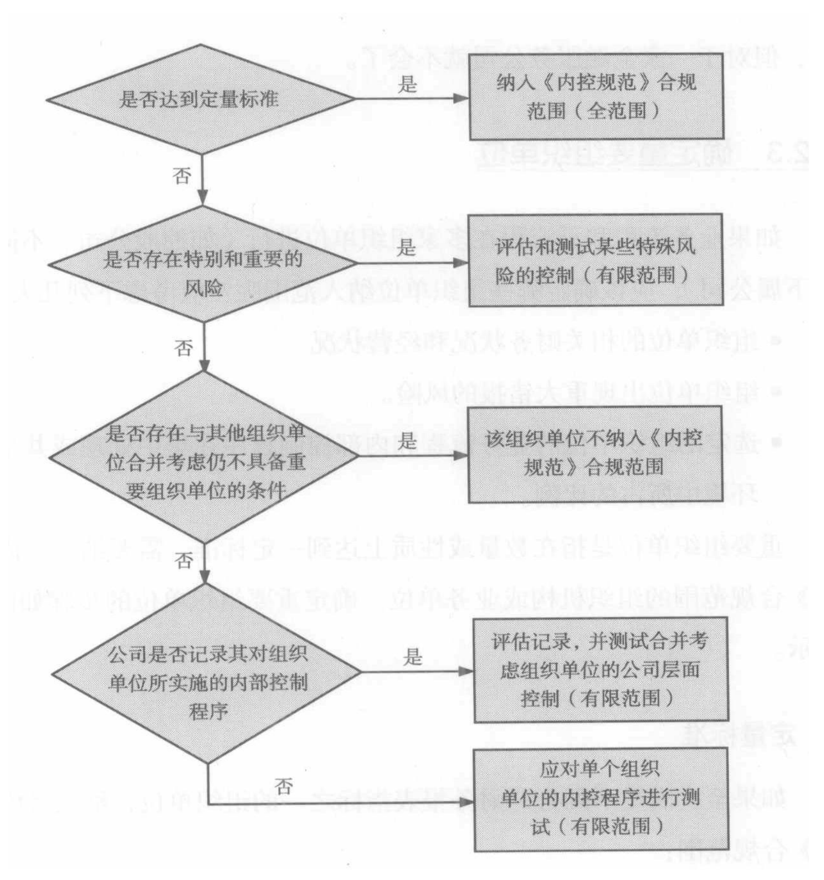


图 3-2　确定重要组织单位的步骤

定量指标应以公布的合并财务报表为出发点。很多公司使用了最近财政年度（如截至 2009 年 12 月 31 日的合并财务报表）或季度（2010 年第 2 季度）的财务信息，但是，在分析过程中采用的财务信息可能随具体财务信息的详细程度和数据的可靠程度有所变化（如年度，季度和月财务信息）。最后，应使用其认为最能代表公司财政年度财务状况的财务信息进行评估。信息可能来自：

- 公司于财政年度末按照各组织单位列示的年度预算。
- 最近财政年度的财务信息。
- 最近季度数据（资产负债表）和最近财政年度的数据（年度损益表）。比如，一家公司以 2010 年 12 月 31 日为财政年度结束日，则可以使用截至 2010 年 6 月 30 日的资产负债表及截至 2009 年 12 月 31 日的损益表数据。

如果选定为信息来源的财务数据受到异常活动或重要交易的影响很大，必须对这些数据进行修改，使这些数据不反映这些活动和交易。还应对任何预算或上一年度的数据进行更新，反映预计未来出现的重大变动。

2. 定性标准

在确认重要组织单位时，先按定量标准进行确认，凡是达到定量标准的，直接纳入《内控规范》合规范围（全范围），对于其他的组织单位，还必须从定性的角度确认是否属于重要组织单位。

尽管某些组织单位对合并财务状况或经营成果的财务重要性可能不大，但这些组织单位负责的某些领域仍有可能存在导致重大错报的风险。对于那些存在可导致重大错报的特殊风险的组织单位（如负责外汇交易或资金运作的组织单位），应记录和测试可降低这些特殊风险的内部控制，并记录将某因素划分为特殊风险的原因。

表明某组织单位在某领域内的风险有所增加的因素包括：

- 管理层的风险评估（参考本书第 2 章内容）。
- 内部或外部审计发现和建议。
- 重要、异常或非重复性交易。
- 单个会计科目余额巨大。

● 管理层的变动。

如果特殊风险所影响的会计科目是重要会计科目，那么这个会计科目在这个组织单位对应的业务流程纳入《内控规范》合规范围。举例如表3-3所示。

表3-3 重要会计科目、组织单位与流程的对应

重要会计科目	组织单位				流程			
	A	B	C	D	销售	采购	资金	财务报告
流动资产								
货币资金	√			√	√	√	√	√
应收账款								
坏账准备								
存货								

特殊风险所影响的会计科目“货币资金”是重要会计科目，那么组织单位A和单位D中的销售、采购、资金和财务报告流程纳入《内控规范》合规范围。

无须对那些本身或与其他组织单位合并考虑都不会对公司的财务报表造成重大错报的组织单位执行进一步的程序。一般来说，这些组织单位加总起来通常不会超过用来确定重要组织单位所定量指标，也不会存在任何特殊的定性风险。

如果几个组织单位合并起来考虑被认为是重要的，应考虑下列因素：

① 如果公司层面的内部控制得到了有效的设计和执行，应记录和测试公司层面的内部控制情况以获得保证。此外，还可以确定是否需要其他证据，如穿行测试、自身评估、内审的审核或监管控制等相关证据，从而得出这些组织单位的控制活动的设计和运行是有效的结论。

② 如果公司层面的内部控制没有得到有效的设计和执行，必须对这些

组织单位的控制活动进行测试，以获得充分的保证，即这些内部控制得到了有效的设计和执行。

如果公司在这些组织单位未设置公司层面的内部控制，或者该内部控制程序不可靠，管理层则应确定在每个组织单位需要执行的程序的性质、时间安排和范围，以获得必要的保证。（公司层面的内部控制将在后面章节具体论述。）

在评估哪些组织单位应进行公司层面的控制的测试和应测试哪些内部控制程序时，该准则指出应考虑下列几个要素：

- 各组织单位相对的财务重要性。
- 由各组织单位引起的重大错报风险。
- 在不同的组织单位中业务运营和对于财务报告的内部控制的相似之处。
- 业务流程和财务报告的集中化程度。
- 控制环境的有效性，尤其是管理层对于向他人授权的直接控制和有效监督各组织单位的活动的能力。
- 在各组织单位进行的交易的性质和数量及相关资产。
- 组织单位出现重大未确认负债的潜在可能性，以及组织单位以公司名义发生负债的程度。
- 管理层的风险评估程序和将某组织单位排除在财务报告的内部控制评估范围之外的分析。

相关链接

出售、并购对合规范围的影响

- 《内控规范》及其配套指引没有明确提及出售、并购对《内控规范》实施范围的影响。

- 一般认为，对于在年度结束前进行的出售，如一家上市公司有意于第二季度末出售其一家大型子公司，管理层可以不对该子公司的内部控制程序进行评估，除非该出售交易未在计划的期间内完成。
- 至于并购对《内控规范》合规范围的影响，目前还没有明确详细的指引。
- 美国《萨班斯法案》关于并购对内部控制范围的影响：美国证券交易委员会指出，如果不可能在收购结束日与管理层内部控制评估日之间对被收购业务进行内部控制评估，那么管理层可以不将新收购的机构纳入其财务报告内部控制评估中。但是免除评估的期间不应超过收购日后一年。如果新收购的机构未被纳入评估，那么管理层必须在其报告中披露该项事实。审计师也可采用同样做法，同样须在审计报告中说明该机构未被纳入评估范围。

3.2.4 识别重要会计科目和披露事项的相关财务报表认定

实施《内控规范》就是明确对公司外部财务报告中重要会计科目和披露事项进行相关财务报表认定的控制程序。为达到这一目标，管理层应从合并财务报表和附注开始（见图 3-1），执行上述每一步骤，并最终明确对应于财务报表认定相关的控制活动和程序，当然也是基于业务流程的目标（主要是财务报告目标）及信息处理目标（主要是与财务报告相关的目标），如图 3-3 所示。

对于每项会计科目和披露事项来说，应确定和记录相关的财务报表认定，并测试与这些财务报表认定有关的内部控制。

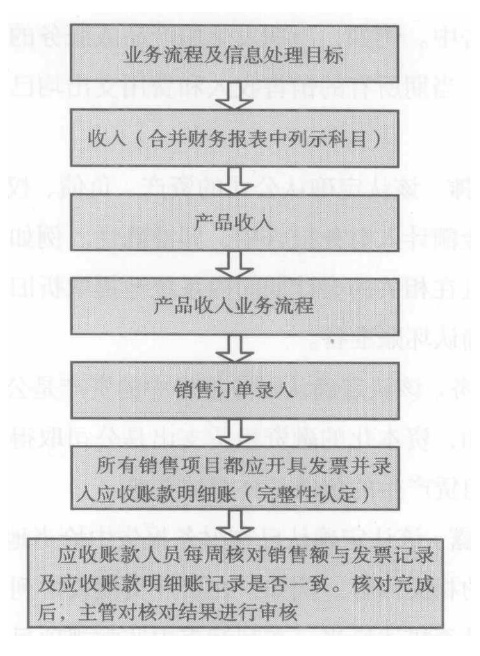


图 3-3　业务流程及其目标、财务报表认定和控制的关系

1. 认定定义及分类

财务报表认定是指管理层对财务报表各组成要素的确认、计量、列报做出的明确或隐含的表达，是评估重大错报风险的基础，包括各类交易、账户余额、列报认定。

1）财务报表认定包括以下几个方面

① 存在或发生。该认定确认公司的资产或负债在财务报告截止日是否存在，入账的交易在财务报告期间是否已经发生。例如，库存商品应是真实存在和可供销售的；销售收入应代表与客户进行了产品交易或提供服务，以获取现金或其他形式报酬。

② 完整性。该认定确认公司所有应在财务报告中记录的交易都已按规

定包括在财务报告中。例如，当期发生的产品或服务的采购都已在财务报告中完整地记录；当期所有的销售收入和费用支出均已全部反映在财务报告中。

③ 估价或分摊。该认定确认公司的资产、负债、权益、收入和费用全部已经按照正确金额计入财务报告中，即准确性。例如，固定资产应按历史成本入账，并且在相关的会计期间内系统地提取折旧；应收账款应按可变现净值计算并确认坏账准备。

④ 权利与义务。该认定确认财务报告中的资产是公司的权利，负债是公司的义务。例如，资本化的融资租赁支出是公司取得对租入资产权利的成本，相应的因租赁产生的负债是公司的义务。

⑤ 表达与披露。该认定确认已在财务报告中恰当地归类、描述和披露各会计科目核算的相关内容。例如，在资产负债表中列为长期借款所涉及的特别约定条款是否描述恰当；在利润表中非常规项目的归类和描述是否恰当。

财务报表认定与每项重要会计科目的相关程度不尽相同。例如，现金科目一般与估价的认定无关，但如果现金中包括外币，则与估价的认定有关；然而，现金科目总是与存在性和完整性的认定相关。此外，内部控制部门可以在期末财务报告流程中，集中考虑表达与披露的认定。

2）对期末账户余额运用的认定（包括但不限于资产负债表）通常分为下列类别

① 存在。记录的资产、负债和所有者权益是存在的。

② 权利和义务。记录的资产由单位拥有或控制，记录的负债是单位应当履行的偿还义务。

③ 完整性。所有应当记录的资产、负债和所有者权益均已记录。

④ 计价和分摊。资产、负债和所有者权益以恰当的金额包括在财务报

表中，与之相关的计价或分摊调整已恰当记录。

3）对各类交易和事项运用的认定（包括但不限于利润表）通常分为下列类别

① 发生。记录的交易和事项已发生，且与单位有关。

② 完整性。所有应当记录的交易和事项均已记录。

③ 准确性。与交易和事项有关的金额及其他数据已恰当记录。

④ 截止。交易和事项已记录于正确的会计期间。

⑤ 分类。交易和事项已记录于恰当的账户。

4）对列报运用的认定（包括但不限于披露）通常分为下列类别

① 发生及权利和义务。披露的交易、事项和其他情况已发生，且与单位有关。

② 完整性。所有应当包括在财务报表中的披露均已包括。

③ 分类和可理解性。财务信息已被恰当地列报和描述，且披露内容表述清楚。

④ 准确性和计价。财务信息和其他信息已公允披露，且金额恰当。

以上内容如表 3-4 所示。

表 3-4 财务报表认定分类

认定\含义	期末账户余额相关	各类交易和事项相关	列报相关
完整性（C）	所有应当记录的资产、负债和所有者权益均已记录	所有应当记录的交易和事项均已记录，交易和事项已记录于正确的会计期间	所有应当包括在财务报表中的披露均已包括
存在与发生/真实性（E）	记录的资产、负债和所有者权益是存在的	记录的交易和事项已发生，且与单位有关，交易和事项已记录于正确的会计期间	披露的交易、事项和其他情况已发生

续表

认定\含义	期末账户余额相关	各类交易和事项相关	列报相关
准确性（A）	不适用	与交易和事项有关的金额及其他数据已恰当记录	财务信息和其他信息已公允披露，且金额恰当
估价或分摊（V）	资产、负债和所有者权益以恰当的金额包括在财务报表中，与之相关的计价或分摊调整已恰当记录	不适当	不适用
权利和义务（O）	记录的资产由单位拥有或控制，记录的负债是被检查单位应当履行的偿还义务	不适当	披露的交易、事项与单位有关
表达和披露（P）	资产、负债和所有者权益已记录于恰当的账户	交易和事项已记录于恰当的账户	财务信息已被恰当地列报和描述，且披露内容表述清楚

2. 判定原则

为准确反映会计报表认定，可以参考以下原则。

① 唯一性原则。为准确认定，按照上述认定定义及分类的内容，只选定一个最相关的科目和一个最相关的认定。假如发现一笔付款的记账凭证会计分录为借方应付账款 101 万元，贷方银行存款 101 万元，而后附的银行贷记凭证上金额为 110 万元，同时还发现该笔 110 万元的付款申请已经相应审批。由于涉及“货币资金、存货、应付账款”三个会计报表项目和“存在和发生（真实性）、表达和披露、估价或分摊（准确性）”三个认定，从上述可以判断，该笔业务不涉及“存货”，而且“应付账款”也由于“货币资金”的对应科目而出现的，真正导致该笔会计分录发生的应该是“货

币资金”，这样就选定对应的会计报表项目为“货币资金”。同时，该笔分录附有完整的原始单据且符合审批要求，说明该笔业务是真实的；会计分录正确，说明表达与披露是正确的。而分录金额与原始单据不符，说明是准确性存在问题。最终我们判定该笔业务影响的就是“存货”会计报表项目的“估价或分摊（准确性）”。

② 相关性原则。会计报表项目大多是由多个会计科目分析填列的，而每个会计科目又分为若干个二级、三个科目，这样一方面会计报表项目可以自上而下追踪到明细科目，另一方面明细科目最终也会自下而上地反映到会计报表项目中去。由于我们采用的是数理统计的随机抽样方法来抽取样本，并采用正态分布的相关理论计算错报金额，如果在抽样时不对样本的范围加以限定，就会导致哪怕是一个明细科目小小的错报同整个会计报表项目的基数相乘后，都会变成一个巨大的数字。经过对会计科目加以分析，绝大多数潜在错报可以计算到一级会计科目，对于需要计算到二级科目的应将有关样本抽全，如应交税金需要计算到其二级科目，则应细化、明确检查底稿抽样要求。

3．常见业务涉及的认定

请参考表3-5所举例子。

表3-5　常见业务涉及的认定举例

常见业务	存在与发生	完整性	权利与义务	估价或分摊	表达和披露
盘点	√	√	√		
账务处理、ERP系统的发票校验[①]	√			√	√
合同、入账原始单据及其审批；价格、信用	√				

续表

常见业务	存在与发生	完整性	权利与义务	估价或分摊	表达和披露
原始单据连号		√			
暂估入账	√	√		√	√
账实核对、账账核对、对账	√	√			
减值准备、折旧[2]	√			√	√
固定资产、存货、借款、债券；代保管[3]			√		
成本费用分摊				√	
账龄分析等计划矩阵披露内容					√

注：① 账务处理本身不涉及真实性，只有控制点描述时有“根据……进行账务处理时”才涉及；而发票校验的重要内容就是三单匹配，因而涉及真实性。

② 表达与披露指是否将原始单据的数据准确地反映在报表上，只在入账环节体现。

③ 权利与义务认定包括所有资产和负债的认定，但基于重要性原则，只对存货、固定资产、无形资产、借款等需要权属认定的项目在取得时确认该认定。

4．单笔业务涉及认定举例

请参考表 3-6 和表 3-7 所举的例子。

表 3-6　与销售收入相关的几项认定举例

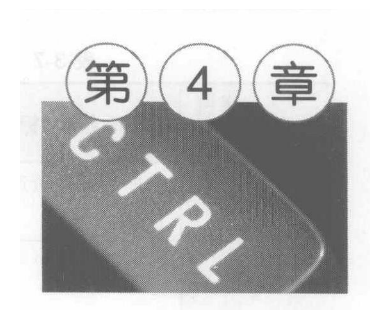
完整性	所有销售交易均已登记入账	发运凭证连续编号，并与销售收入明细账核对一致
存在与发生/真实性	销售交易均适当审批 登记入账的销售交易是真实存在的	建立客户信用评价制度，及销售交易授权审批制度，并严格执行 记录销售收入时审查所附详细凭证
估价或分摊	登记入账的销售交易正确计价	在登记销售收入时将销售收入上的数量与发运凭证上的记录进行比较核对

续表

表达和披露	登记入账的销售交易分类恰当	将登记入账的销售交易原始凭证与会计科目表比较核对

表 3-7　与固定资产相关的几项认定举例

举例 认定	内部控制目标举例	内部控制举例
完整性	所有固定资产都已记录	建立并严格执行固定资产定期盘点制度，并对固定资产盘盈盘亏的结果跟踪处理
存在与发生/真实性	账上记录的固定资产确实真实存在	建立并严格执行资本性支出授权审批制度；所有固定资产的取得和处置均需经企业管理层的书面确认 设置总账、明细账、固定资产登记卡；按类别、使用部门、每项固定资产进行明细分类核算；增减变化均有原始凭证
权利和义务	所在固定资产均为单位所有	取得或处置固定资产签订合同，办理产权交易手续，取得或转移权属证明
估价或分摊	账上记录的固定资产金额准确，正确反映固定资产的价值	定期对资产状况进行检查分析，因市价持续下跌或技术陈旧、损坏、长期闲置等原因导致其可收回金额低于账面价值的，应将可收回金额低于账面净值的差额作为固定资产减值准备。减值数额需经适当审核并及时计提入账，并根据上级审定结果及时调整
表达和披露	确保按相关规定计提折旧，保证固定资产和累计折旧的准确性	财务部门按照公司确定的固定资产分类、使用年限计提固定资产折旧；财务部门负责人审核本级分公司的折旧提取是否正确。财务部监督下属公司固定资产折旧的提取情况



内部控制体系建设

4.1 内部控制体系建设概述

4.1.1 内部控制体系建设组织体系

对于绝大多数公司来说，为保证《内控规范》顺利实施而执行的程序将十分重要和复杂。《内控规范》的范围远远超过一个公司的财务部门所能涵盖的工作范围，将触及公司的各个重要领域，如生产、销售、研发、IT、税务、法律及内部审计等几乎公司所有职能领域。《内控规范》不只是财务或内部审计部门的事，管理层还将与第三方进行更加广泛的合作，如外部审计师、利益相关方（供应商、客户）、咨询顾问（如有）等。

同时内部控制体系建设的完成将需要投入大量的时间和公司资源。

确定内部控制体系建设组织架构尤为重要。在《内控规范》合规的头一年，我们建议采用项目管理办公室（Project Management Office, PMO）的办法。在董事会及审计委员会的领导下，由公司高层（通常是首席执行官/CEO、首席财务官/CFO）担任“内部控制建设项目”负责人，在其领导下成立“内部控制建设项目指导委员会”（Steering Committee），全面负责协调整个项目的顺利实施。该委员会应从各主要相关部门选出代表，这些部门主要包括财务部门、IT 部门、业务部门（销售、研发、生产等）、法务部门和内审部门等；在该委员会下有一个具体操作部门，一般是内审部门，或者单独成立内部控制部门来推动内部控制建设。

对于具有多个业务单位或业务覆盖地区广泛的大型公司来说，按照公司业务单位或地域进行划分，遵循公司的整体组织结构，建立类似的机构，并向总部“内部控制建设项目指导委员会”汇报工作。例如，按照业务地

域划分的公司可以采用如图 4-1 所示架构设置。

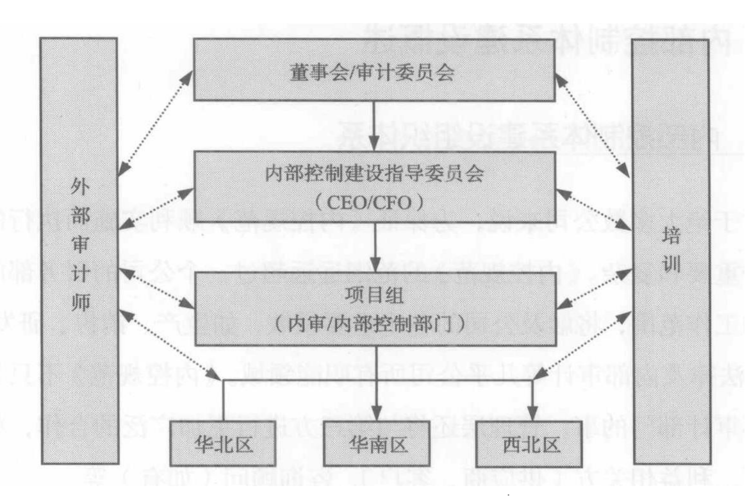


图 4-1　内部控制体系建设工作组织体系

从图 4-1 可以看出，在项目组织架构的各个层面，基于合规的要求，我们都与外部审计师保持良好的沟通和互动，同时培训也将贯穿始终。本书第 5 章将更深入介绍内部控制组织体系与培训方面的内容。


相关链接

一些经验与教训分享

- **内审部门的定位。**尽管内审部门充分参与《内控规范》实施项目是自然而然的事情，但它同样必须关注内控规范项目中没有涉及的公司的其他风险。如果由内审部门承担内控规范项目的主要责任，那么内审的常规职能将可能因为没有资源和时间被搁置。
- **厘清责任。**《内控规范》项目很大程度上与财务报告相关，但并不等于业务流程负责人都来自财务部门，如正确确认收入的关键要素之一是与客户签订适当的合同。公司应在政策中具体说明这些

要素，但确保达标的最终责任和执行相应内部控制程序的责任很可能落在公司销售部门身上。

- **与外部审计师的互动。**为了确保公司内部控制审计的顺利通过，公司管理层（内部控制建设项目指导委员会）定期与其外部审计师召开会议，沟通项目进展及出现的问题，实现双方工作的协调性，以保证项目效率与效果。

4.1.2 内部控制体系建设的内容

内部控制建设按风险及控制所作用的层面的不同，分为公司层面控制、IT 一般控制、业务层面控制和 IT 应用控制四个方面的建设，它们的关系如图 4-2 所示。

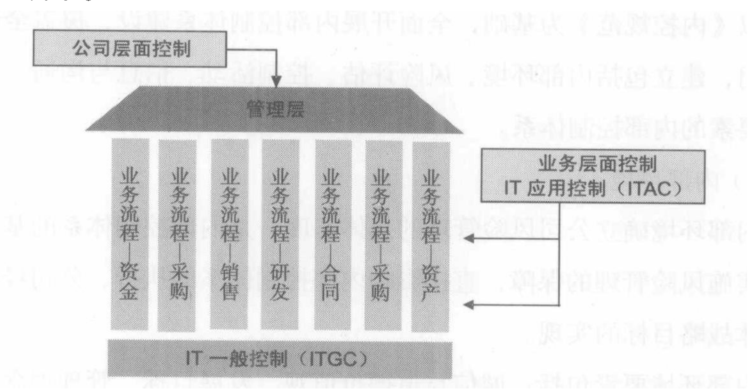


图 4-2 各层面控制的关系

内部控制建设过程主要包括启动、试点、推广实施、测试完善四个阶段。

1. 公司层面控制建设

公司层面控制是管理层确保在公司内部各个领域获得适当、有效控制

的重要机制，主要包括：公司层面风险评估、公司层面控制建设。

（1）公司层面风险评估

风险识别：公司针对确定关键事项，从外部环境及内部环境两个角度，通过关键成功因素的分析，考虑和寻找在实现目标过程中内外部风险。

风险分析：判断风险重要性水平，形成公司层面风险数据库。

风险应对：针对已识别的公司层面风险，对现有控制进行有效性、充分性分析，通过规范统一或者重新设计，确定并实施其中的关键控制，形成完整统一的公司层面风险管理的策略、机制、重要标准、关键过程程序及重大的改进措施。

具体内容请参考本书第 2 章。

（2）公司层面控制建设内容

以《内控规范》为基础，全面开展内部控制体系建设，覆盖全部业务和部门，建立包括内部环境、风险评估、控制活动、信息与沟通、内部监督五要素的内部控制体系。

1）内部环境

内部环境确立公司风险管理的总体态度，是内部控制体系的基础，是有效实施风险管理的保障，直接影响内部控制体系的执行、公司经营目标及整体战略目标的实现。

内部环境要素包括：诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及审计委员会、组织结构、权利和责任的分配、人力资源政策与措施、员工胜任能力、反舞弊机制等内容。

2）风险评估

风险评估是识别及分析影响公司目标实现的风险的过程，是风险管理的基础。在风险评估中，管理层应识别和分析对实现目标具有阻碍作用的

业务层面和公司层面的风险，明确在重要会计科目、披露事项和相关财务报表认定中产生重大错报的风险。

风险评估主要经过目标制定、风险识别、风险分析、风险反应四项基本程序。

3）控制活动

控制活动是确保管理层关于风险应对方案得以贯彻执行的政策和程序。控制活动存在于公司所有级别的分支机构和职能部门，包括授权、批准、查证、核对、报告、内部审计、重大风险预警、企业法律顾问、经营业绩评价和资产保全措施等活动。

控制活动重点关注针对公司的每项业务活动都要有必要和恰当的政策和程序，已确定的控制行为能得到恰当的执行。

4）信息与沟通

信息与沟通的构成要素包括信息、沟通、IT 一般控制、IT 应用控制和信息披露等。其中信息是指来源于公司内、外部，与公司经营相关的财务及非财务信息。沟通是指信息在公司内部各层次、各部门，以及在公司与客户、供应商、监管者和股东等外部环境之间的传递。

公司应建立有效的 IT 一般控制、IT 应用控制并监督执行。

5）内部监督

内部监督是管理层对公司内部控制体系有效性进行持续评估的过程，包括：持续监督、独立评估和缺陷报告三要素。

2. IT 一般控制建设

IT 一般控制（IT General Control，ITGC）是内部控制建设的一个重要组成部分，它所指的是内部控制中对信息系统相关部分的控制，保证由信

息系统支持的流程控制是可靠的、生成的数据和报告是可信的。IT 一般控制涉及了 IT 管理和运营的各个方面。

IT 一般控制建设的内容包括：控制环境、信息安全、项目建设管理、系统变更管理、信息系统日常运作、最终用户操作等，具体为：

① 控制环境。包括信息系统总体控制环境、信息与沟通、风险评估、监控等。

② 信息安全。包括信息安全管理组织、逻辑安全、物理安全、网络安全、计算机病毒防护、第三方安全管理、信息安全事件响应等。

③ 项目建设管理。包括项目建设方法论、项目立项审批、商业软件及硬件的外购、项目启动、项目需求分析、项目设计、系统开发实施、系统测试、数据移植、系统上线、项目验收和上线后评估、用户培训等。

④ 系统变更管理。包括变更管理、日常变更流程、紧急变更流程等。

⑤ 信息系统日常运作。包括机房环境控制、系统日常运作监控、批处理作业调度管理、备份与恢复、问题管理等。

⑥ 最终用户操作。包括最终用户计算机操作安全制度、电子表格管理等。

3. 业务层面控制建设

业务层面控制建设的主要内容是针对业务活动层面风险，以公司层面控制政策为导向，规范业务流程，制定业务活动层面风险控制措施。

业务层面控制建设的主要内容有：

（1）业务流程梳理

业务流程梳理就是按照一定的架构，将企业各项业务活动、相关要素及其关联性以业务流程的形式反映出来。通过流程梳理可以将各项业务活动与岗位设置、岗位职责、工作制度等诸因素结合起来，是识别风险、分

析控制措施及分析风险管理水平，进行流程管理、内部控制建设及 ERP 建设的前提。

（2）业务流程描述

业务流程的描述形式有文本法、表格法和图形法等。根据公司实际采用的方法，流程描述要素应包括：业务流程名称编码和起止点、工作步骤、业务风险点、控制要求、工作界面，以及对应的组织机构、岗位和记录表单等。

（3）风险控制矩阵

1）风险评估

风险评估是识别及分析影响公司目标实现的因素的过程，是风险管理的基础。主要经过目标设定、风险识别、风险分析、风险反应四项基本程序，识别出业务活动中存在的风险。业务活动层面风险主要包括经营风险、合规性风险和财务报告风险等。

2）风险数据库建立

风险数据库是进行风险记录的工具。风险数据库记录整个公司业务范围内存在的风险，按照流程，记录各个流程中可能出现的风险，并对风险的属性进行记录。风险按影响结果分为经营决策风险、违反法律法规风险、财务报告失真风险、资产安全受到威胁风险、营私舞弊风险五类；按重要性程度分为关键风险和一般风险；按照其反映的内容分为公司层面风险和业务活动层面风险。

3）风险控制矩阵编制

风险控制矩阵（Risk Control Matrix, RCM）用来详细地体现业务流程中存在的风险和控制措施设计的情况。它是对现有规章制度进行描述和分析的主要载体，也是联结业务流程、风险、现有控制措施、规章制度文件的工具。

4）差异分析与完善

差异分析主要是找出制度差异的类型和具体原因，评估制度文件的完整性。评估制度文件完整性，应从谁负责执行控制、什么时候、多久执行控制、控制的具体内容、控制的实施证据五要素角度进行，如果缺乏其中某些要素则为控制文件不完善。主要有缺少文件规定的差异和文件规定不完善的差异。

通过差异分析，对有风险无控制的，要先建立控制；对有控制但不完善的，要完善控制。

5）关键控制确认

① 确认关键控制的基本标准。关键控制确认是在全面进行风险评估、控制分析的基础上，为了强化控制活动，突出控制重点，简化评估测试而开展的一项重要工作。因此为了确保关键控制的确认结果准确无误，确认关键控制的基本标准是关键。

② 确认关键控制的程序指导。确认关键控制，需要经过识别、修改、征求意见、审批等严格的程序，确保关键控制的准确。

4．IT应用控制建设

（1）应用系统的划分

信息应用系统按对公司业务流程的影响程度划分为重要应用系统、普通应用系统和其他应用系统。

1）重要应用系统

这类应用系统与内部控制直接相关的应用系统，需要满足以下条件：在公司范围内普遍使用；存在对财务报告产生重大影响的会计科目，或存在对财务报告产生重大影响的功能，或与财务系统存在接口（手工或自动）；

在重大方面无法依赖手工控制。

2）普通应用系统

这类应用系统是与内部控制间接相关的应用系统，不存在对财务报告产生重大影响的功能；不存在对财务报告产生重大影响的会计科目；在公司范围内不普遍使用；所有重大方面可以依赖手工控制。

3）其他应用系统

重要应用系统与普通应用系统以外的应用系统划分为其他应用系统。

（2）应用系统权限管理

应用系统权限管理包括访问控制和职责分离。

① 访问控制是指用户能够访问哪些应用系统内的资源或执行哪些任务（或功能）的范围，从控制的角度考虑在系统中所拥有的功能权限和数据权限是否超出了其工作需要。

② 职责分离是把一个业务（子）流程的工作内容分为几个职责不相容的部分并由不同的人来完成，避免因同一个人能够操作不相容职责而产生的舞弊风险。

（3）应用系统自动控制

信息系统可利用数据类型校验、重复输入校验、批总量控制、序列校验、系统匹配、逐一检测、编辑校对、预定的数据列表、授权检查、有效性检查等技术控制，对应用系统的输入、处理和输出进行有效控制。

4.1.3 内部控制建设过程

内部控制建设可以分为四个阶段[①]，如图 4-3 所示。

① 主要针对那些下属公司众多、业务复杂的大型企业集团。规模较小、业务简单的中小型企业，无须采用这种先试点后推广的做法。

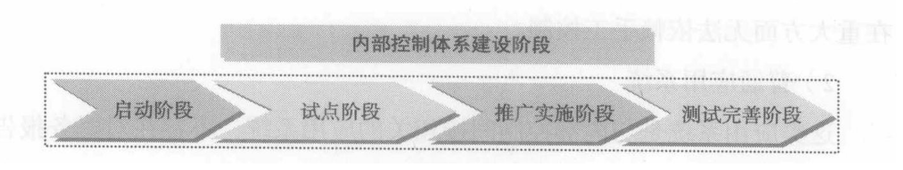


图 4-3　内部控制建设阶段

1．启动阶段

启动阶段一般在总部进行，主要是明确建设目标，确定组织架构和工作机制，现状分析，人员培训，收集相关法规标准和可借鉴的经验，确定总体阶段及内容和工作计划，如图 4-4 所示。

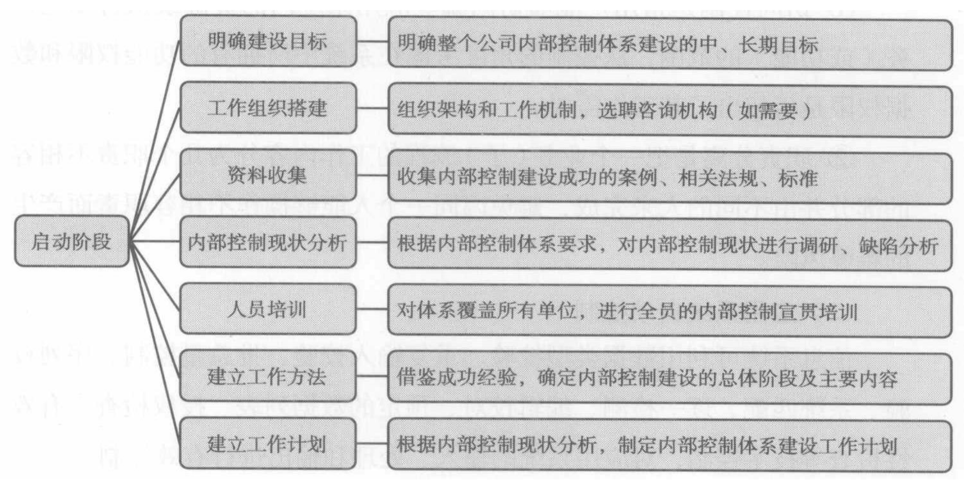


图 4-4　启动阶段工作内容

2．试点阶段

对于大型企业，下属公司繁多，可以采取先试点、后推广的方法。主要是通过在总部及试点单位进行现状描述和风险评估，明确内部控制建设

的内容，主要包括公司层面、业务（流程）层面和IT（信息系统）层面三大板块，初步完成内部控制设计，如图4-5所示。

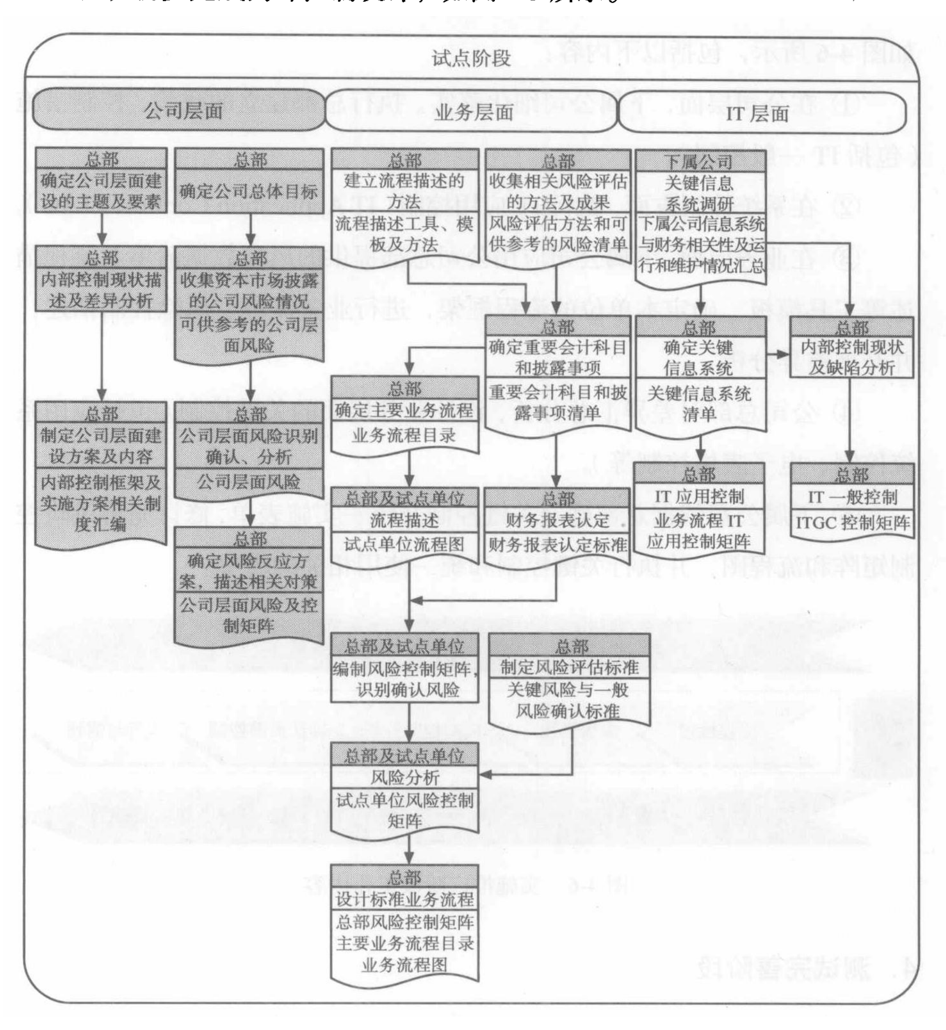


图4-5 试点阶段工作内容

3．推广实施阶段

这个阶段要在所有纳入内部控制建设范围的组织单位全面推广展开，如图 4-6 所示，包括以下内容：

① 在公司层面，下属公司细化落实、执行总部建立的政策、控制措施（包括 IT 一般控制）。

② 在系统控制方面，执行 IT 应用控制（IT Application Control，ITAC）。

③ 在业务层面，下属公司应用公司总部提供的风险数据清单及流程描述等工具模板，确定本单位的流程框架，进行业务流程、风险控制描述，并开展差异分析。

④ 公司总部对差异汇总分析，设计业务层面的关键控制（包括应用系统控制、电子表格控制等）。

⑤ 下属公司依据总部确定关键控制及统一实施表单，修订完善风险控制矩阵和流程图，并执行关键控制和统一使用相关的表单。

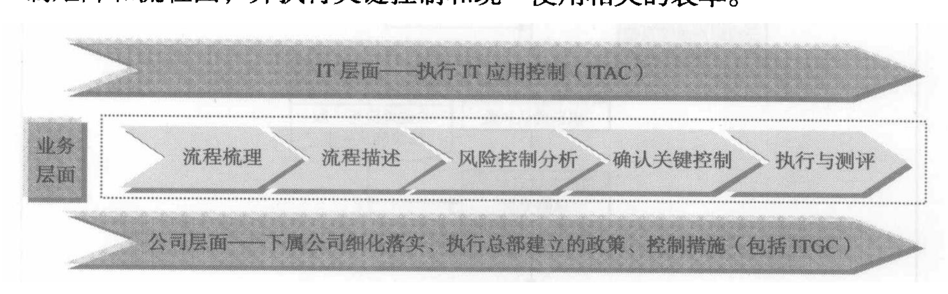


图 4-6　实施推广阶段工作内容

4．测试完善阶段

在下属公司对关键控制的执行效果进行测试，做出评价，整改缺陷，不断完善内部控制体系，如图 4-7 所示。

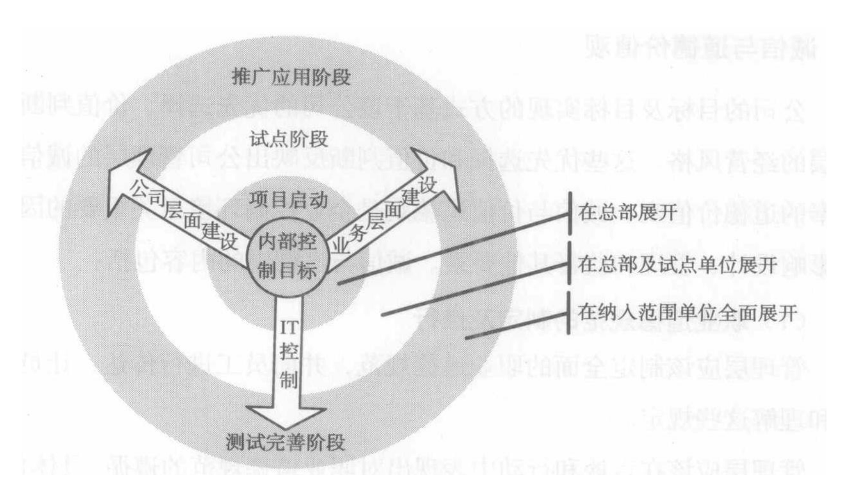


图 4-7　测试完善阶段工作内容

4.2 公司层面内部控制建设

以《内控规范》为依据，全面开展内部控制体系建设，建立包括内部环境、风险评估、控制活动、信息与沟通、内部监督五要素的内部控制体系。

4.2.1 内部环境

内部环境是内部控制体系的基础，是有效实施内部控制的保障，直接影响着公司内部控制的贯彻执行、公司经营目标及整体战略目标的实现。内部环境确定了公司的总体态度，是内部控制所有其他组成要素的基础。

内部环境包括诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及审计委员会与监事会、组织结构、权利和责任分配、人力资源政策与措施、员工胜任能力、反舞弊机制 10 项内容。

1．诚信与道德价值观

公司的目标及目标实现的方式基于该公司的优先选择、价值判断和管理层的经营风格。这些优先选择和价值判断反映出公司管理层的诚信及其信奉的道德价值观。诚信与价值道德观是企业控制环境至关重要的因素，它影响设计、管理和监督其他要素。诚信与道德观的内容包括：

（1）职业道德规范的制定及推行

管理层应该制定全面的职业道德规范，并向员工进行传达，让员工熟知和理解这些规定。

管理层应该在言谈和行动中表现出对职业道德规范的遵循。具体包括：

① 职业道德规范的内容是全面的，并针对利益冲突、非法或其他不当付款、不正当竞争、内幕交易等做出规定。

② 公司对职业道德规范进行有效的宣传推广。

③ 员工知晓什么行为是可接受的，什么是不可接受的，以及当遇到不当行为时应该采取的行动。

相关链接

道德规范（摘要）

1. 诚实与道德行为。每位员工必须以个人最高标准与职业道德行事，并且不能对企图欺骗或逃避责任行为坐视不理。员工履行公司职责时，其必须以诚实和道德作为行事准则。对于某一行为是否诚实与道德产生疑问时，所有员工都应根据情况，从直接上级或高级管理层寻求咨询。

2. 利益冲突。当员工的个人利益与公司利益相背时，就会导致利益冲突。任何员工应当积极避免任何现实或潜在的利益冲突，须以公司的利益为重，绝不允许出于个人利益的考虑而损害公司的利益。每位员工有责任向公司披露可能是直接或间接利益冲突的情形，包括因个人或家

庭成员与其他商业团体或组织机构的关系，对公司或公司的业务带来的利益影响。

3. 索求、接受与馈赠。

① 索求。公司及其下属公司的员工严禁利用职权向公司的客户、经销商、供应商及任何与公司业务相关的个人或团体索求礼物，包括礼品、贷款、小费、奖金、职务、协议、服务和帮助。

② 接受。任何员工应避免接受任何可能使其难以客观工作或影响其从公司利益出发行事的礼物。同样，任何使人质疑公司公正及合理立场的礼物，亦应予以拒绝。主动赠予的礼物能否接受，以下原则可作为标准：

— 不会影响受赠者的工作业绩。

— 受赠者不会感到有义务向赠予者做出回报。

— 受赠者能毫无保留地完全公开所接受的礼物。

— 赠予出于正常的商业性质，如因广告、促销或商业惯例赠予的礼品、节日期间的压岁钱等。

— 礼物的金额不高，如不超过20美元，拒绝这样的小礼物会视为不和气、不礼貌。

③ 馈赠。任何员工在任何时候不得向任何个人或团体馈赠或行贿，谋取不正当的商业利益，妨碍其在合同、招标及拍卖下做出公正的判断。

4. 内幕交易。内部信息包括任何未公开的、一般被投资者视为投资决策重要依据的信息，无论这些信息是否有利，如尚未发布的财务状况，对于结盟或企业单位或重大资产的买卖等其他重大事项，诉讼或有关某项业务的其他重大事实等。因雇用关系或董事在公司董事会的任用而获得的信息不得用于谋取利益或者借此向其他人要求收取“小费”，除非这些信息之前已经公开，并且即使在这种情况下，披露这些信息也应得到其他必要批准。

5. 不正当竞争。公司公平和诚实地超越其竞争者。公司不寻求通过非法和不道德商业手段，谋取竞争优势。每个涉及人员应尽力公平对待公司的客户、服务提供商、供应商、竞争者和员工。任何人员不得通过暗箱操作、隐瞒、滥用特权、失实陈述或任何不公平的交易手段取得对别人的不公平优势。

6. 解释与违纪处理。如果对自己的行为是否违反了本准则存有疑虑，可通过电话（电话号码）、电子邮箱（E-mail 地址）或与法务部门联系寻求解释、澄清及指导。任何不遵守本准则的违纪行为将受到相应的纪律处分，包括解除劳动合同，甚或诉讼当地司法机关。

7. 举报。举报者可以通过实名或匿名方式对违反本规范的行为进行举报。公司鼓励举报者在对违规操作进行举报时表明身份，使公司获取更多信息，在必要时可再次联系举报者。举报者可通过以下任何一种方式举报：通信地址（包括邮编）；电话/传真号码；电子邮件地址等。

（2）“高层管理基调”的建立

“高层管理基调”的建立包括有详尽的道德指导和在公司上下进行充分沟通指导。具体包括：

① 管理层通过一言一行，在公司范围内传达对职业道德规范的遵循。

② 员工感觉到被同仁敦促做正确事情的压力。

③ 管理层对存在问题的迹象予以适当关注。

（3）与利益相关方的关系

管理层与员工、供应商、客户、投资者、债权人、保险公司、竞争对象和审计师等进行交往时，应当遵守职业道德规范，并且要求其他人同样遵守道德标准，与客户、供应商、员工和其他相关方的日常业务建立在诚实和公允的基础上。



（4）违规处理

针对违反政策和道德标准的情况及时采取适当的措施。具体包括：

① 管理层对公司的违规行为应进行回应。

② 对违规行为进行处理，处理的原则和结果应在公司上下进行传达。

③ 员工确信如果违规要承担后果。

（5）管理层对干预或逾越既定控制的态度

① 管理层就需要进行干预的情形和进行干预的频率订立方针制度。

② 管理层对控制制度的干预被适当地记录和解释。

③ 明确禁止管理人员逾越既定控制。

以上所提到的“干预”是指为了合法的目的而偏离既定的规章和程序的行为，当出现特殊的和非标准的交易和事件时，管理层的干预是合理的；“越权”是指为了不合法的目的而不遵守既定的规定和程序。

（6）实现目标的压力

绩效目标，特别是短期目标的确定是合理的；薪酬与绩效目标的实现挂钩程度是合理的。具体包括：

① 不存在偏激的奖惩制度，影响员工对道德标准的遵守。

② 升职和薪金不能仅基于短期绩效目标的实现。

③ 实施控制以减少其他形式存在的诱惑。

2. 发展目标

公司的发展目标是风险评估的基础和依据。管理层结合公司自身的实际情况制定战略目标，在此基础上制定相关的经营目标、报告目标和合规性目标，并且根据企业自身的发展目标来确定风险，采取必要的行动对这些风险进行管理。

① 战略目标：与公司的总目标息息相关，支持公司完成其使命的目标。

② 经营目标：以资源利用的效率和效果为中心，防止公司因灾害性风险或人为失误而遭受重大损失的目标。

③ 报告目标：以经营管理和对外披露所需信息的可靠性为中心，防止公司因信息的错报、漏报而遭受损失的目标。

④ 合规性目标：以适用法律和法规的遵循性为中心，防止公司因违反相关法律、法规而遭受损失的目标。

公司的发展目标可以分为公司和业务活动两个层面。公司层面目标是指公司的总目标和相关的战略计划，以资源的分配和优先利用为中心。业务活动层面目标可以视为总目标的子目标，是针对公司业务和管理活动而制定的更加专门化的目标。

（1）公司层面的目标

公司要实现有效控制首先要建立目标。公司层面的目标包括对公司期望实现目标的总体说明，并辅以相关的战略计划做支撑。

① 公司层面的目标应与企业战略规划息息相关，并贴近企业实际，不泛泛而论，对公司期望达到的主要目标进行充分指导和说明。

② 公司层面目标应及时向管理层及员工进行传达。

③ 公司计划和预算与公司层面目标、战略计划及当前情况保持一致。

（2）业务活动层面的目标

① 业务活动层面的目标源于公司的总体目标和战略规划，并与之相联系。业务活动层面的目标随着不同时期、不同任务而不断变化。这些目标应针对每个重要活动制定，同时，各目标之间需保持一致，即业务活动层面的目标与公司层面目标及战略计划保持一致；各业务活动层面目标之间保持一致。业务活动层面目标与所有重要业务流程相关，应具体、明确、

可度量，并有充分的资源保证目标的实现。

② 在业务活动层面目标的制定过程中，各级管理层参与的程度及他们对目标的负责程度对目标的实现会产生直接影响。

③ 公司应识别业务层面目标中对公司层面目标产生影响的重要因素，以采取恰当措施保证公司层面目标的顺利实现。

3. 管理理念与企业文化

管理层的管理理念和企业文化影响公司的管理方式，包括对各种风险的态度。在财务报告内部控制方面，管理层的管理理念和企业文化主要表现在管理层对财务报告的态度，如会计政策的选择是否合理，会计核算时是否遵循谨慎性原则，对待数据处理、会计职能及人事管理方面的态度等。例如，坏账准备的计提方法有账龄分析法、余额百分比法、个别认定法，公司采用了账龄分析法与个别认定法相结合的方法。管理理念与企业文化包括：

（1）公司接受业务风险的态度

① 在介入新业务前，是否经过仔细的风险和收益分析后才采取行动。

② 是否经常介入风险特别高的业务，还是在接受风险方面非常保守。

（2）关键人员的更换频率

关键部门人员（如经营、会计和数据处理等部门）的更换频率，具体包括：

① 管理层和监督层人员是否存在过高的更换频率。

② 关键岗位员工是否存在突然辞职，或辞职提前通知期较短的现象。

（3）管理层对数据处理、财务报告等的态度

管理层对数据处理和会计职能的态度，以及对财务报告和资产安全可

靠性的关注程度。具体包括：

① 管理层看待财务职能的方式及给予的授权。例如，认为财务部门仅仅是公司的“掌柜”，还是经营管理活动的控制中心。

② 所选用的会计准则是否追求财务报告利润最高。

③ 企事业单位财务负责人是否对报告结果签字确认。

④ 基层单位的财务部门是否与总部的财务部门有工作汇报关系。

⑤ 重大资产，如现金、票据等是否存在很好的保护措施，防止未经授权的接触。

（4）高级管理人员相互交流的频率

高级管理人员和各级业务部门管理人员相互交流的频率，特别是在双方处于不同的地域时。具体包括：

① 高级管理人员是否经常走访调研企事业单位。

② 是否经常召开专业性的管理层会议，加强信息的交流。

4. 风险管理策略

公司应围绕自身的发展战略，通过确定风险容量、风险承受度、内部控制有效性标准，来体现公司内部控制的总体策略，并据此制定风险反应方案。

公司依据发展战略确定风险容量，以体现公司在战略制定与实施过程中愿意承受的风险范围和风险水平，反映公司的风险偏好。公司针对特定目标，制定具体的风险承受度，体现在实现特定目标过程中公司对差异的接受程度。公司确定风险容量和风险承受度时，要正确认识和把握风险与收益的平衡，防止忽视风险而片面追求收益，或者单纯为规避风险而放弃发展机遇的情况。风险承受度与风险容量需保持一致。

5. 董事会及审计委员会与监事会

考虑到管理层可能逾越内部控制，一个积极有效的董事会及审计委员会与监事会，能够起到重要的监督作用。在确保有效的内部控制方面，董事会及审计委员会与监事会起到至关重要的作用。

（1）独立性

董事会和监事会独立于管理层，可以对管理层的决策提出建设性的必要的质疑。具体包括：

① 对管理层的决定（如经营决策、重大交易）进行推断并提出质疑，对经营结果进行质询（如预算执行差异）。

② 有权询问和详查公司的经营活动，提出不同观点，并在认为必要时采取适当的行动。

（2）审计委员会

建立董事会审计委员会，他们在专业和资历方面能够有效地处理相关的重要问题。审计委员会由公司独立董事组成并由其中一位担任主任委员，其中至少有1名具有会计审计或相关财务管理专长的成员。

（3）董事的学识和经验

董事具有足以履行其职责的知识和经验。具体包括：董事拥有足够的知识、行业经验和时间，从而有效地开展工作。

（4）与内、外部审计师的会面频率和时间

① 审计委员会单独与首席财务官（CFO）、会计人员、内部审计师和外部审计师会面的频率和时间，对讨论财务报告流程、内部控制与企业风险管理体系，以及管理层绩效的合理性等提出重大意见和建议。

② 董事会/审计委员会和监事会每年审核内部和外部审计师的工作范围。

（5）及时充分地获得信息

为董事会/审计委员会和监事会及时充分地提供信息，以便其及时监督管理层的目标和战略、公司的财务状况和经营成果，以及重大协议的条款等。具体包括：

① 董事会定期收到关键信息，如财务报告、主要的市场变化趋势、重大合同和谈判信息。

② 董事相信其得到了适当的信息。

（6）获知和调查不正当行为

为董事会及审计委员会提供充分、及时的信息，以便及时获知敏感信息、调查、不当行为（如重大的法律诉讼、监管机构调查、贪污、挪用公款、滥用公司财产、违反内部人员交易法规、非法支付等）。具体包括：

① 存在告知董事会重大问题的程序。

② 及时沟通信息。

（7）薪酬政策的监控

监控高级管理人员和内部审计部门负责人的薪酬，聘用和终止上述高级管理人员的雇用。具体包括：

① 薪酬委员会批准所有管理层与绩效挂钩的激励计划。

② 薪酬委员会在咨询审计委员会意见的前提下，确定内部审计负责人的薪酬和任免事宜。

（8）建立适当的“高层基调”

高层基调（Tone of The Top）主要是指公司管理层的诚信和道德价值观等。具体包括：

① 董事会及审计委员与监事会充分参与、评价“高层基调”的有效性。

② 董事会及审计委员与监事会采取行动以保证适当的“高层基调”。

③ 董事会及审计委员与监事会明确地强调管理层应该遵守的行为准则。

（9）监督管理层对审计发现的跟进

董事会及审计委员于监事会依据其发现，采取适当的措施，包括专项调查。具体包括：

① 向管理层就需要采取的具体行动下达指令。

② 如果需要，进行监督和跟踪处理。

6．组织结构

公司的组织结构提供了公司为实现目标，对公司的活动进行规划、执行、控制和监督的架构。通过组织结构，确定权限与职责的关键领域和建立适当的报告机制。

公司根据自身的需要来确定其组织结构，公司组织结构的适当性在相当程度上取决于公司的规模及其活动的性质。组织结构的内容包括：

（1）组织结构适应信息流通和权力集中程度

① 公司组织结构的适当性，如组织结构是否有利于信息的上传、下达和在各业务活动间的传递。

② 考虑公司经营业务的性质，如公司的组织结构按照适当集中或分散的管理方式设置。

（2）关键管理人员的知识和经验

关键管理人员应具备执行其职责的知识和经验，并接受适当培训。

（3）汇报机制的适当性

组织结构确立的汇报机制是有效的，能确保管理人员之间有通畅的沟通渠道。

（4）组织结构变化的适应性

组织结构在某种程度上应随环境的变化而变化，并根据变化的业务或行业环境来评价公司的组织结构。

7. 权利与责任分配

对于组织内的全部活动，是否合理有效地分配了职责和权限，并为执行任务和承担职责的组织成员特别是关键岗位的人员，提供和配备所需的资源，并确保他们的经验和知识与职责权限相匹配。要使所有员工知道他们的职责和权限。具体包括：

（1）职责和职权进行了分配

要根据公司的目标、经营职能和监管要求，分配责任和授权，包括信息系统的责任和变化的授权。具体包括：职权和职责被授予公司内的员工；对员工进行授权和分配职责时，应充分考虑适当的信息；职权和职责要相对应。

（2）关键岗位人员的知识和技能充分

关键岗位人员主要指数据处理和会计职能部门的员工，其应具备与公司规模、业务活动和信息系统相适应的知识和技能水平；拥有足够的员工以完成其职责。

（3）责任分配与授权是恰当的

① 完成工作所需的权力与高级管理人员参与的程度应存在适当的平衡。

② 授予合适级别的员工纠正问题或实施改进的权力，并且此授权也明确了所需的能力水平和权力界限。

8. 人力资源政策与措施

人力资源政策是对员工聘用、定岗、培训、评价、晋升、考核、薪酬等方面的制度规定，它引导员工达到公司期望的职业道德水平和胜任能力。具体包括：

（1）人力资源政策和程序

制定有雇佣、培训、晋升和员工薪酬的政策及程序，该政策和程序可以招聘并发展有能力、可信的人员，能够支持有效的内部控制体系；对招聘和培训合适人员的关注程度是适当的。

（2）员工责任和目标

员工（包括新员工）应清楚地知道他们的工作职责及公司对他们的期望。

（3）违规行为的纠正措施

对违背政策和程序的行为的处理，包括管理层对工作失职采取适当的处理措施；对违背政策的行为有适当的纠正措施；对员工进行教育，使其明白错误的行为。

（4）道德标准的遵从

将对职业道德规范的遵从作为对员工进行评价的一项标准。

（5）对候选人的背景进行核查

核查候选人的背景，特别要考虑公司不能接受的行为或活动，重点对频繁更换工作和职业背景相差很大的候选人要仔细核查，包括对犯罪记录的调查。

9. 员工胜任能力

员工胜任能力就是反映员工完成工作任务所需的知识和技能。工作任

务需要具备什么样的知识和技能的员工来完成，通常是管理层根据公司的目标和实现这些目标的战略和计划，在胜任能力和成本之间进行平衡后做出的决策。员工胜任能力内容包括：

（1）岗位职责描述

管理层应对各岗位进行职责描述，定义各岗位的具体工作任务、职责和权限等。

（2）分析胜任工作所需的知识和技能

管理层应分析并确定员工胜任工作所需的基本知识和技能，并有证据表明员工具备工作所需的基本知识和技能。

10．反舞弊机制

（1）舞弊的概念及特征

舞弊是指以故意的行为获得不当或非法的利益。舞弊行为主要有两个特征：一是主观故意；二是获得不当或非法利益，包括对财务报告造成重大影响或给公司造成重大损失等情况。比如，以不适当的收入确认方法调节收入、高估资产或低估负债；商业行贿、对政府行贿、其他不当付款等。

（2）反舞弊机制关注的内容

管理层有效地设计、实施公司反舞弊程序和控制，针对规避财务报告内部控制的行为和其他欺诈行为，采取适当的措施。

① 董事会及审计委员会与监事会监督公司反舞弊程序和控制。

② 建立并推行道德准则。

③ 建立投诉举报机制。

④ 雇用和晋升时进行背景调查。

⑤ 建立舞弊调查程序并实施恰当的补救措施。

⑥ 进行舞弊风险评估。

⑦ 为减少已识别的舞弊风险应该设计并实施有效的控制活动。

⑧ 对反舞弊相关信息进行收集和分享并适当培训。

⑨ 管理层对反舞弊程序和控制的质量持续监控和定期评估。

相关链接

反舞弊守则（摘要）

- 目标。此反舞弊机制的主要目标是防止舞弊，加强公司的管治与内部控制，规范商业行为，维护公司的诚信商业交易，建立公司员工和公众对存在潜在相反分歧的可疑舞弊或贪污可依的程序及保护措施，并实现利于公司股东合法的经营目标，诚实与道德行为。
- 适用范围。此反舞弊机制适用于公司及其附属公司。
- 舞弊的概念及形式（略）。
- 舞弊的预防和控制（略）。
- 舞弊案件的受理、调查、报告（略）。
- 投诉举报渠道。通信地址（包括邮编）；电话/传真号码；电子邮件地址等。
- 对舞弊行为的处理。根据违规行为的情节轻重，处以通报批评，降职，降薪，解除劳动合同关系等；返还获取的不正当利益，赔偿公司所遭受的损失等；对涉嫌犯罪的人员，移送司法机关处理；对于打击报复者，从严处置；对于目的不纯的虚假举报，干扰公司正常运作甚至构成诽谤的，严肃处理或移送司法机关处理。

4.2.2 风险评估

本书第 2 章对风险评估做了详细介绍，第 3 章对财务报告风险评估做

了比较详细的说明，本部分主要从制度层面介绍风险评估。

1．培育风险管理文化

企业文化是指一个企业长期形成的一种稳定的文化传统，它是企业员工共同的价值观、思想信念、行为准则、道德规范的总和。它的实质是企业的经营理念、价值观和企业精神。企业文化是一个企业在长期生产经营中倡导、积累，经过筛选提炼成的，是企业的灵魂和潜在的生产力，是打造企业核心竞争力的战略举措。

建立具有风险防范意识的企业文化，促进企业风险管理水平、员工风险管理素质的提升，保障企业风险管理目标的实现，是公司企业文化建设的一项重要内容。将风险管理文化建设融入企业文化建设全过程，大力培育和塑造良好的风险管理文化，树立正确的风险管理理念，增强员工的风险管理意识，使风险管理成为员工的共识和自觉行动，促进企业建立系统、规范、高效的风险管理机制。

2．建立风险评估机制

公司开展持续性的风险评估工作，在公司内部建立通用的风险管理语言和标准，明确风险承受度。

企业应当报据设定的控制目标，结合不同发展阶段和业务拓展情况，全面系统持续地收集与风险变化相关的信息，如历史事件的记录、相关的调查和分析资料、现有控制和制度等信息和资料。另外拓展其他的信息来源，包括但不限于实践和相关的经验，市场、行业调查和分析，经济、工程或其他模型，专家判断等。

根据收集的信息，结合企业实际情况，及时进行风险评估，及时调整

风险应对策略。

公司定期或有以下情况之一发生时，应及时组织进行风险评估：

① 内部控制体系建立。

② 新产品开发。

③ 新业务介入。

④ 新系统应用。

⑤ 内部控制政策和目标修改。

⑥ 业务流程发生较大变化。

⑦ 组织机构变革。

⑧ 法律法规、监管要求发生变化。

⑨ 经济周期性波动。

⑩ 行业发生变革。

⑪ 同业发生新的案例。

⑫ 其他认为需要进行风险评估的情况。

4.2.3 控制活动

1. 控制活动的概念

控制活动是确保管理层关于风险应对方案得以贯彻执行的政策和程序。控制活动存在于公司所有级别的分支机构和职能部门，包括授权、批准、查证、核对、报告、内部审计、重大风险预警、经营业绩评价和资产保全措施等活动。

（1）控制活动的一般方法

控制活动通常包括：不相容职务分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制、绩效考评控制和信息系

统控制等。

1）不相容职务分离控制

要求企业全面系统地分析、梳理业务流程中所涉及的不相容职务，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制。

企业在确定职责分工过程中，应当充分考虑不相容职务相互分离的制衡要求。不相容职务通常包括：授权、批准、业务经办、会计记录、财产保管、稽核检查等。

不相容职务主要有：

- 授权进行某项经济业务和执行该项业务的职务要分离，如有权决定或审批采购的人员不能同时兼任采购员职务。
- 执行某些经济业务和审核这些经济业务的职务要分离，如填写销售发票的人员不能兼任审核人员。
- 执行某项经济业务和记录该项业务的职务要分离，如销货人员不能同时兼任会计记账工作。
- 保管某些财产物资和对其进行记录的职务要分离，如会计部门的出纳员与记账人员要分离，不能同时兼任。
- 保管某些财产物资和核对实存数与账存数的职务要分离。
- 记录明细账和记录总账的职务要分离。
- 记录日记账和登记总账的职务要分离。

2）授权审批控制

要求企业根据常规授权和特别授权的规定，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。

授权一般包括常规授权和特别授权。常规授权是指企业在日常经营管理活动中按照既定的职责和程序进行的授权。特别授权是指企业在特殊情

况、特定条件下进行的授权。企业应当编制常规授权的权限指引，规范特别授权的范围、权限、程序和责任，严格控制特别授权。

企业各级管理人员应当在授权范围内行使职权和承担责任，业务经办人员必须在授权范围内办理业务。未经授权的部门和人员，不得办理企业各类经济业务与事项。

企业对于重大的业务和事项（对于金额重大、重要性高、技术性强、影响范围广的经济业务与事项），应当实行集体决策审批或者联签制度，任何个人不得单独进行决策或者擅自改变集体决策。

3）会计系统控制

要求企业严格执行国家统一的会计准则制度，加强会计基础工作，明确会计凭证、会计账簿和财务会计报告的处理程序，保证会计资料真实完整。

企业应当依法设置会计机构，配备会计从业人员。从事会计工作的人员，必须取得会计从业资格证书。会计机构负责人应当具备会计师以上专业技术职务资格。

4）财产保护控制

要求企业建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全。企业应当严格限制未经授权的人员接触和处置财产。

5）预算控制

要求企业实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束。及时分析和控制预算差异，采取改进措施，确保预算的执行。

6）运营分析控制

要求企业建立运营情况分析制度，经理层应当综合运用生产、购销、投

资、筹资、财务等方面的信息，通过因素分析、对比分析、趋势分析等方法，定期开展运营情况分析，发现存在的问题，及时查明原因并加以改进。

7）绩效考评控制

要求企业建立和实施绩效考评制度，科学设置考核指标体系，对企业内部各责任单位和全体员工的业绩进行定期考核和客观评价，将考评结果作为确定员工薪酬及职务晋升、评优、降级、调岗、辞退等的依据，强化对各部门和员工的激励与约束。

8）信息系统控制

要求企业结合实际情况和计算机IT应用程度，建立与本企业经营管理业务相适应的信息化控制流程，提高业务处理效率，减少和消除人为操纵因素，同时加强对IT信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制，保证信息系统安全、有效运用。

2. 控制活动的分类

控制活动的分类有多种划分标准，归纳起来主要有以下分类方法。

（1）控制活动按影响的范围分类

分为公司层面控制活动和业务层面控制活动两种。

① 公司层面控制活动，是管理层确保在公司内部各个领域获得适当、有效控制的重要机制，包括控制环境范围内的内部控制、反舞弊程序与控制、风险评估流程、集中化的处理和程序、监督、期末财务报告流程、统一的规章制度等。

② 业务层面控制活动，直接作用于公司生产经营业务活动的具体控制，也称业务控制，如业务处理程序中的批准与授权、审核与复核，以及为保证资产安全而采用的限制接近等控制。



（2）控制活动按作用分类

分为预防性控制和发现性控制两种。

① 预防性控制，是指为防止错误和非法行为的发生，或尽量减少其发生机会所进行的一种控制。例如，岗位职责分工、合同需要经过审批、办理业务须经有关人员批准等。

② 发现性控制，是指为及时查明已发生的错误和非法行为，或增强发现错误和非法行为机会的能力所进行的各项控制。例如，编制银行存款余额调节表、财产清查、核对账目等。

（3）控制活动按手段分类

分为人工控制和自动控制两种。

① 人工控制，是以人工方式执行的控制。例如，财务报告必须由企业负责人和总会计师签字并盖章，原始凭证上必须有经办人员的签字等。

② 自动控制，是由计算机等系统自动执行的控制。例如，禁止未授权的用户登录系统，系统自动的账目核对等。

（4）控制活动按重要程度分类

分为关键控制和一般控制两种。

① 关键控制，是在相关业务流程中影响力和控制力相对较强的一项或多项控制，其控制作用是必不可少和不可替代的。如果缺少该项控制，将在很大程度上直接导致重大风险的发生。

② 一般控制，只能发挥局部作用，影响特定范围的控制。

图 4-8 是一个关于控制活动例子。

3．控制活动重点关注的内容

① 针对公司的每项业务活动都有必要和恰当的政策和程序。

② 已确定的控制行为得到恰当的执行，强调内部控制的执行。

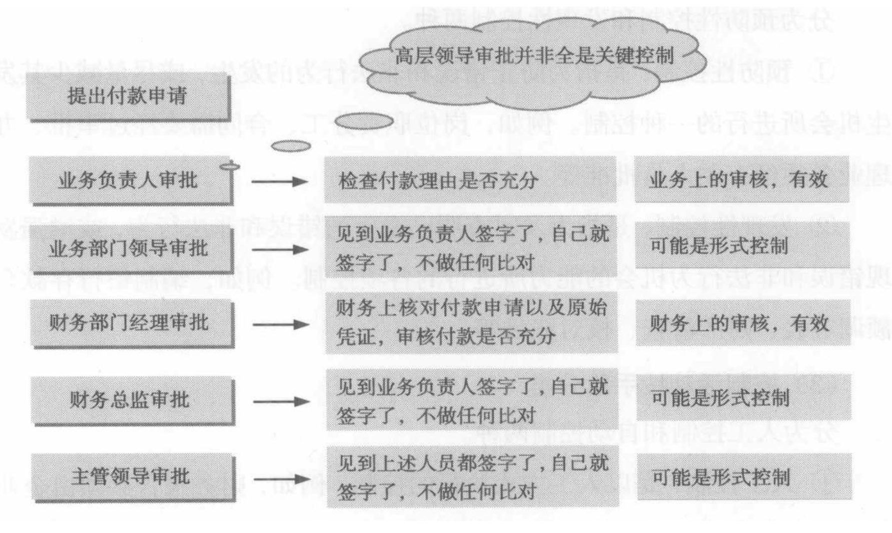


图 4-8　控制活动举例

4.2.4　信息与沟通

信息与沟通是公司经营管理所需的信息被识别、获取并以一定形式及时传递，以便员工履行职责，包括信息、沟通、IT 一般控制、IT 应用控制和信息披露等。

1. 信息

（1）信息的概念

信息是指来源于公司内、外部，与公司经营相关的财务及非财务信息，包括从外部获取的行业、经济、监管信息，以及内部产生的经营管理、财务等方面的信息。信息必须及时、准确地传递给需要的人，以帮助其行使各自的控制和其他职能。

（2）信息的内容

按信息来源不同，可将公司的信息分为内部信息和外部信息。

① 内部信息主要包括财务信息、经营信息、规章制度信息、综合信息等。

内部信息的获取渠道主要有：机关职能部门的文件、调研报告；财务会计报告；信息收集、反映的情况；群众来信来访、员工直接向上级沟通的信息；内部刊物、资料；公司局域网；各种会议提案、记录、纪要等。

② 外部信息主要包括国家法律法规、国内外监管机构信息，以及客户、供应商、竞争对手的信息等。

外部信息的获取渠道主要有：国家部委和外部监管方的文件；期刊；中介机构；因特网；广播、电视；公司采购及销售部门收集的市场和价格信息；驻外办事处提供的信息；外部来信来访；参加行业会议、座谈交流等多种渠道。

（3）信息重点关注的内容

① 建立获取信息的机制。公司应该建立获取外部相关信息的机制，以随时掌握有关市场状况、竞争对手的动态、立法或监管的要求及经营环境的变化等。

② 及时向相关人员汇报足够的信息。各级管理人员能够及时得到并分析信息，以便判断需要采取什么措施。

③ 建立 IT 总体规划。指定专门部门负责识别不断产生的信息需求，订立与战略决策相联系的长期 IT 总体规划。

④ 管理层对信息系统的支持态度。为建立或改进信息系统提供足够的、必要的资源，包括但不限于管理人员、分析人员、具备必要能力的编程人员控制措施。

2. 沟通

（1）沟通的概念

沟通是指信息在公司内部各层次、各部门，以及在公司与客户、供应商、监管者和股东等外部环境之间的传递。建立横向和纵向相互通畅、贯穿整个公司的信息沟通渠道，确保公司目标、风险策略、风险现状、控制措施、员工职责、经营状况、市场变化等各种信息在公司内部得到有效的传达；与公司的相关方如供应商、客户、律师、股东、监管机构、外部审计师，就相关信息进行必要的外部沟通。

（2）沟通的内容

建立有效沟通，公司需要从沟通环境、沟通渠道、沟通方式及沟通反馈多方面进行建设。

有效沟通的特点表现为：

① 沟通频率高、方式随意。

② 沟通深入且平等。

③ 具有沟通所需的物质条件。

④ 完善的沟通制度和系统。

⑤ 全方位的信息共享。

（3）沟通重点关注的内容

① 向员工传达其职责和控制责任的有效性。包括沟通方式应能实现沟通的目的；员工应清楚他们的行为要达到的目标，以及他们的工作对于实现这些目标有什么作用；员工应清楚自己的职责与他人的职责如何相互影响。

② 公司内部是否充分交流。包括企业内部沟通的充分性，信息的完整性和及时性，以及使员工履行职责所需信息的充足性。

③ 沟通渠道应开放有效。包括公司应存在与所有有关方面的反馈机

制，并对相关方的建议、投诉和收到的其他情况建立记录并得到有效处理；必要的信息应向上级汇报并采取相应的跟进措施。

④ 外部相关方了解公司职业道德规范的程度。包括与外部的重要信息交流应由相应的管理人员进行；供应商、客户和其他方面应清楚公司在与其往来的活动中，员工应遵循的职业道德规范；在与外部的日常交往中公司强调员工应遵循的职业道德规范；其他公司员工的不当行为应向适当人员汇报。

⑤ 管理层收到外部信息后应采取及时和适当的应对措施。包括公司应善于接受他人就产品、服务或其他方面反映的问题，并且对这些信息采取适当的汇报或处理措施；在与客户交易或财务记录中出现的错误应得到及时的纠正，并且就产生错误的根源进行调查和纠正；应由经授权的当事人以外的人员处理收到的投诉，并采取适当的行为与原始信息提供者进行跟踪和沟通；管理层应清楚投诉的性质及数量。

3．IT 一般控制

（1）IT 一般控制概念

IT 一般控制是指适用于企业在 IT 的开发、实施、运行、维护及管理等方面的控制，它可以更好地保护企业的信息资产，可以提高信息系统对业务的支撑力度，增强企业信息系统的运行效力。IT 一般控制简称 ITGC（IT General Control）。

（2）IT 一般控制的内容

IT 一般控制通常包括控制环境、信息安全、项目建设管理、系统变更管理、信息系统日常运作、最终用户操作等。

① 控制环境包括总体控制环境、信息与沟通、风险评估、监控等。

② 信息安全包括信息安全管理组织、逻辑安全、物理安全、网络安全、计算机病毒防护、第三方安全管理等。

③ 项目建设管理包括项目立项审批、项目建设方法论、项目管理等。

④ 系统变更管理包括变更管理、日常变更流程、紧急变更流程等。

⑤ 信息系统日常运作包括机房环境控制、系统日常运作监控、批处理作业调度管理、备份与恢复、问题管理等。

⑥ 最终用户操作包括最终用户计算机操作安全制度、电子表格管理等。

4. IT 应用控制

（1）IT 应用控制的概念

IT 应用控制（IT Application Control，ITAC）包括应用软件中的电算化步骤，以及用于控制不同种类交易处理的相关手工操作程序。这些控制结合在一起，可以保证系统中的财务和其他信息的安全性、完整性、准确性和有效性。

（2）IT 应用控制的内容

IT 应用控制通常包括业务流程中使用的信息系统（如 ERP 系统）所涵盖的控制。

（3）IT 应用控制重点关注内容

① 完整性。包括所有的交易都经过处理，且只处理一次；不允许数据的重复录入和处理；例外情况的发现和解决。

② 准确性。包括所有的数据（包括金额和账户）是正确和合理的；例外情况被及时发现以保证交易被记录在正确的会计期间。

③ 有效性。包括交易被适当授权；系统不接受虚假交易；例外情况被

发现和处理。

④ 接触控制。包括未经授权，不得对数据进行修改；数据的保密性；物理设备的保护等。

5. 信息披露

信息披露是指公司为确保符合监管机构的监管要求，向所有市场参与者和监管部门提供及时、有序、一致、准确、完整、可靠和可信的公司信息。

4.2.5 内部监督

1. 监督的概念

监督是对内部控制体系有效性进行评估的持续过程，包括持续监督、独立评估和缺陷报告等要素。通俗地讲，监督就是对内部控制体系的设计和执行是否有效进行检查的过程。

2. 监督的内容

对内部控制体系设计与执行情况的检查的形式有持续监督、独立评估和缺陷报告三个要素。

（1）持续监督

持续监督是在公司日常经营过程中进行的，包括日常的管理和监督活动，以及员工在履行职责时所采取的检查内部控制执行质量的行为。

通俗地讲，持续监督就是对内部控制体系的日常管理、监督、比较、核对和其他常规性活动。以下行为均属于持续监督的内容：

① 管理层在履行其日常的管理活动时，对营运报告、财务报告与他们

所得到的资料有大偏离时，可对报告提出质疑。

② 来自外界团体的沟通，可以验证内部信息的正确性，并能及时反映问题的所在。

③ 适当的组织机构及监督活动，可用来辨识缺失。

④ 各个职务的分离，使不同员工之间可以彼此相互检查，以防止舞弊。

⑤ 把信息系统所记录的资料同实际资产核对。

⑥ 定期要求员工陈述他们是否了解企业的行为准则，并加以遵守，对于负责业务和财务的员工，则要求他们陈述某些特定控制是否都予以执行，管理阶层或内部稽核人员还必须验证这些陈述是否确实等。

（2）独立评估

独立评估就是独立于控制活动之外而采取的定期评估行为。

通俗地讲，独立评估就是对内部控制体系设计和执行的有效性进行检查测试的活动，如公司组织的自我测试、公司总部组织的管理层测试和外部审计师的测试等。

（3）缺陷报告

缺陷报告是将内部控制缺陷自下而上报告的行为。缺陷报告要求：及时汇集和报告发现的内部控制缺陷、汇报机制的适当性、跟进评估的适当性等。监督三要素的关系可用图 4-9 表示。

持续监督的有效性程度越高，单独评估的需要程度就越低。

（4）持续监督重点关注的内容

① 内部控制体系运行与维护管理。

② 在日常活动中获得执行内部控制的证据。

③ 外部反映对内部信息的印证程度。

④ 定期核对财务系统数据与实物资产。

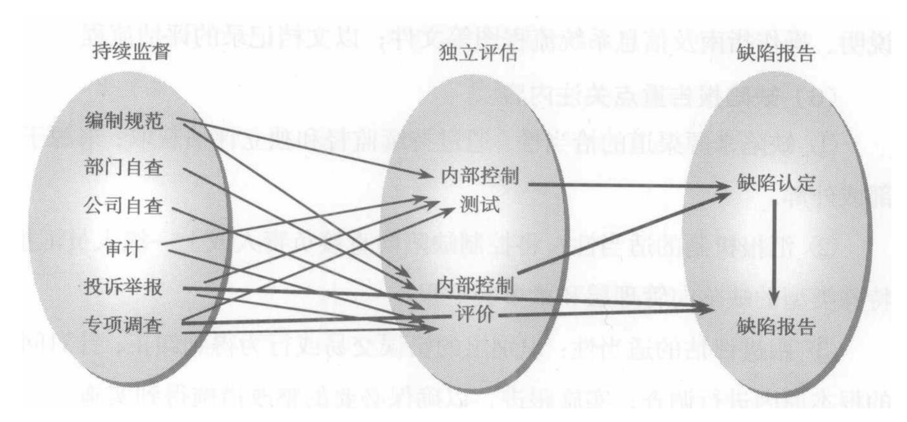


图 4-9　监督三要素

⑤ 对内外部审计师提出的关于加强内部控制的措施做出响应。

⑥ 培训、会议等对内部控制有效性的反馈。

⑦ 定期询问员工是否理解并执行公司的职业道德规范，员工是否执行了内部控制活动。

⑧ 内部审计活动的有效性。

（5）独立评估重点关注的内容

① 独立评估范围和频率：对内部控制体系适当的部分进行评估；评估是由具备必要技能的人员进行的；评估的范围、覆盖的深度和频率是足够的。

② 独立评估过程：评估过程由具有必要职权的高级管理人员主持；测试人员充分地了解公司的活动；了解内部控制体系应该如何运作，以及实际的运作情况；将评估结果与已建立的标准进行对照，并对其进行分析。

③ 独立评估方法：评估方法使用核对清单、问卷或其他一些辅助工具；评估小组共同安排评估程序，并确保各方的努力协调一致。

④ 独立评估所需文档记录：具备书面的政策手册、组织结构图、工作

说明、操作指南及信息系统流程图等文件；以文档记录的评估流程。

（6）缺陷报告重点关注内容

① 缺陷来源渠道的恰当性：通过持续监督和独立评估获取；来源于内部或外部。

② 汇报机制的适当性：将控制缺陷向直接负责人或上一级人员汇报；特殊类型的缺陷向管理层和董事会汇报。

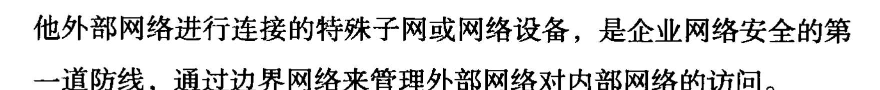
③ 跟进评估的适当性：识别出的错误交易或行为得到纠正；针对问题的根本原因进行调查；实施跟进，以确保必要的整改措施得到实施。

4.3 IT 一般控制建设

根据 IT 一般控制控制目标，IT 一般控制包括控制环境、信息安全、项目建设管理、系统变更管理、信息系统日常运作、最终用户操作六方面内容。

因为涉及一些专业名词，先在此进行名词解释。

- IT 部门。指总部 IT 部门、下属公司 IT 部门。
- 应用系统管理员。指具有应用系统管理员权限，能进行应用系统日常维护和管理操作的人员，一般是 IT 部门人员。
- 应用系统负责人。指对该应用系统的日常管理活动进行授权和决策的人员，以确保应用系统的准确、稳定、安全、可靠运行，并能满足业务需求，一般是该系统主要使用部门的关键用户。
- 信息安全管理负责人。指负责公司信息安全工作的组织、落实、独立审核、监督和检查的人员，属于 IT 部门人员。
- 边界网络。指用于企业内部网络与 Internet、合作伙伴企业网络或其



他外部网络进行连接的特殊子网或网络设备，是企业网络安全的第一道防线，通过边界网络来管理外部网络对内部网络的访问。

- 电子表格负责人。指对电子表格进行日常管理的人员，以保证电子表格完整、准确、安全、可靠，并能满足业务需求。

4.3.1 控制环境

1. IT 总体规划

① 公司 IT 部门应根据业务需要，组织制定公司 IT 总体规划，并报经公司管理层（或者信息化委员会、信息化办公室之类的机构）审批通过后下发执行。

② IT 总体规划应包括 IT 项目建设的规划、相应基础设施建设规划、IT 组织机构设置及人员配备等方面内容。

③ 公司 IT 部门应定期（至少每年度）组织相关业务部门对 IT 总体规划的执行情况及其对公司业务的适应性进行审阅。如果规划执行情况与规划偏离，或规划内容和公司业务实际情况不再适应，管理层应随之调整规划以适应公司业务发展需要。规划的调整应报经公司管理层（或者信息化委员会、信息化办公室之类的机构）审批通过后下发执行。

④ 各下属公司 IT 部门应根据本公司的业务需要，结合 IT 总体规划，制定本单位的 IT 年度工作计划。

⑤ 上述各项工作的文档记录均应归档，其中公司 IT 部门负责 IT 总体规划及其定期审阅和调整文档的归档，下属公司 IT 部门负责本下属公司 IT 年度工作计划的归档。

2．IT组织架构及人力资源管理

公司IT部门作为公司IT建设的牵头部门，负责指导、监督各业务部门、专业公司及下属公司的IT工作。具体表现为：

（1）纵向汇报、沟通、监控机制

① 各级IT部门每年对公司IT部门进行年度工作汇报。

② 公司IT部门不定期对各级IT部门的工作情况进行检查，形成相关文档，如会议纪要或者工作检查报告等，并负责相关文档的归档。

（2）职责分离要求

各级IT部门的岗位设置应考虑安全、内部控制和职责分离的要求。

在进行岗位职责定义时，应注意以下IT管理方面的职责分离要求：

① 制度执行监督者应独立于日常的制度执行者。

② 信息系统管理活动的操作者和授权者不应为同一人。

③ 应用系统管理员和数据库管理员不应为同一人。

④ 程序开发人员不应具备对生产环境的访问权限。

（3）备份机制

各级IT部门在重要工作岗位上可设置两个以上员工互为备份，同时应加强备份岗位和人员的交叉培训。

（4）IT培训计划

各级IT部门应制定针对本企业IT部门员工及普通员工的IT培训计划，做好培训工作，并负责培训计划和所有培训记录的归档。

3．信息与沟通

（1）信息分类

信息分类的目标是确保企业的信息资产得到恰当的保护，信息分类的

过程就是标识信息的类别，确认信息的保护级别。各级 IT 部门应对所属单位使用的信息资产建立清单、进行分级，明确各信息资产的相关责任人。

① 建立《信息资产清单》。

② 按信息资产的重要性和敏感性，将信息资产分为高、中、低三个级别。

③ 将信息资产明确资产责任人，负责信息资产的日常管理。

④ 根据信息资产的变动情况，更新《信息资产清单》。

（2）信息沟通

① 公司 IT 部门及各级 IT 部门负责在本单位进行各项 IT 管理政策、制度和标准的宣贯工作，明确各级 IT 管理者的 IT 内部控制职责。

② 各级 IT 部门应定期评估 IT 管理政策、制度和标准在本单位的执行情况，对于所发现的问题应分析其原因，制定相应的补救措施，并向公司 IT 部门汇报。

③ 以上活动的实施部门负责活动相关文档的归档，如会议纪要、培训记录等。

4. 风险评估

（1）评估公司及业务层面的主要 IT 风险

公司 IT 部门应对公司及业务层面的主要 IT 风险进行评估。

① 分析主要 IT 威胁的影响程度和发生概率。

② 制定相应的风险防范措施。

③ 对剩余风险进行评估。

（2）定期审阅 IT 风险评估结果

公司 IT 部门负责定期（每年）审阅 IT 风险评估结果。

（3）评估由变动引起的风险

当发生重大的 IT 应用或者组织结构变动时，公司 IT 部门应对变动情况进行风险评估，必要时调整相关风险防范措施。

5. 监控

① 各级 IT 部门按照 IT 一般控制的要求进行日常检查与监控，确保 IT 一般控制体系的有效运行。

② 公司 IT 部门每年应对公司范围内的 IT 一般控制执行情况组织测试工作，进行相应监督。

③ 各级 IT 部门每年应对各自单位的 IT 一般控制执行情况进行总结，并向公司 IT 部门提交报告，报告内容包括 IT 一般控制年度执行情况、改进建议等。公司 IT 部门对报告进行审阅，并根据审阅结果确定改进建议。

④ 上述各项工作的文档记录均应归档，各级 IT 部门负责本单位的 IT 一般控制执行情况报告、测试文档和改进建议等相关文档的归档。

4.3.2 信息安全

1. 信息安全管理组织

（1）信息安全管理机制

在公司和下属公司设立信息安全管理负责人，信息安全管理负责人可以由 IT 部门内相关人员兼任，但要确保职责分离。

信息安全管理负责人的职责主要是对 IT 日常工作进行安全监督和检查，因此，信息安全管理负责人不应兼任 IT 日常事务执行等工作。

信息安全管理负责人的主要职责包括：

① 在公司 IT 及信息安全总体规定框架下，负责信息安全规定与标准在本单位的宣贯。

② 负责本单位的信息安全日常工作（包括逻辑安全、网络安全、信息安全事件响应等）的监督和检查。

③ 负责定期（比如每半年）审核本单位 IT 一般控制活动的职责分离状况，填写《职责分离检查表》，将不符情况报相关负责人。

④ 向上级单位信息安全管理负责人进行日常工作汇报和重大事项的专报。

⑤ 负责组织本单位信息安全的培训工作。

（2）员工信息安全培训要求

各级 IT 部门对员工进行信息安全教育和培训，以确认其具有基本的信息安全意识，对信息安全培训结果要书面记录并归档。培训内容主要包括：

① 对网络管理员、操作系统管理员、应用系统管理员、数据库管理员等相关人员应开展必要的信息安全技术培训，使这些员工了解、掌握网络、服务器、应用系统、数据库、个人计算机等信息资产的必要信息安全知识。

② 在信息安全规定、标准发生重大调整时，应组织相关培训，使员工及时了解、掌握变更内容。

③ 在应用系统的新建、升级对用户使用产生影响时，应事先开展必要的培训，使相关员工了解系统变更所带来的信息安全权限和责任的变化。

（3）员工被要求签署遵守企业的信息安全规定的声明

① 员工签署的聘用合同或保密协议中应包含员工遵守企业信息安全规定声明。

② 人事部门负责员工签署的遵守企业信息安全规定声明的归档。

2．逻辑安全

（1）系统登录验证机制

对操作系统、数据库和应用系统的访问应通过安全的登录程序完成访问信息服务。登录程序应符合下述要求：提供访问控制机制，以确保系统不会被未经授权的人访问、修改或删除信息；应提供身份验证方法。

（2）用户账号管理

1）用户账号分配规则

系统所有用户都应拥有个人专用的唯一账号，以便操作能够追溯到具体责任人，不应在应用系统中设立无人使用的账号。

2）普通用户账号管理

A．用户账号增加流程

- 根据业务需要增加用户账号时，申请人应填写《用户账号及权限管理表》。
- 申请人主管领导确认该用户的岗位职责，同时审批《用户账号及权限管理表》。
- 应用系统负责人审核《用户账号及权限管理表》，根据申请人主管领导所确定的申请人岗位职责分配相应的权限，并签字确认。
- 应用系统管理员根据《用户账号及权限管理表》创建用户，签字确认后通知该用户，并负责《用户账号及权限管理表》的归档。

B．用户权限修改和变更流程

- 用户因工作岗位调动或其他原因需要变更权限时，应填写《用户账号及权限管理表》。

- 用户主管领导确认该用户新的岗位职责，并审批《用户账号及权限管理表》。
- 应用系统负责人审核《用户账号及权限管理表》，根据用户主管领导所确定的新岗位职责，分配相应的用户权限，并签字确认。
- 应用系统管理员根据《用户账号及权限管理表》变更该用户权限，签字确认后通知该用户，并负责《用户账号及权限管理表》的归档。

C．用户权限撤销流程

- 员工因离职或其他原因需要撤销权限时，其主管领导填写《用户账号及权限管理表》，并立即通知应用系统负责人撤销该员工账号的访问权限。
- 应用系统负责人审阅《用户账号及权限管理表》，并签字确认。
- 应用系统管理员根据《用户账号及权限管理表》撤销该账号在所有系统的访问权限，关闭用户账号，并签字确认。
- 应用系统管理员负责《用户账号及权限管理表》的归档。
- 如果离职用户涉及上级业务部门应用系统的用户权限，则通知该应用系统在本单位的主管业务部门，再由本单位的主管业务部门通知上级的主管业务部门撤销该账号在该应用系统的访问权限，并关闭用户账号。

D．特权用户账号管理

① 特权用户包括应用系统管理员、数据库管理员、操作系统管理员、网络管理员等及其他拥有特权的用户。

② 特权用户登记管理：

- 应用系统负责人对应用系统管理员、数据库管理员、操作系统管理员等特权用户及其联系方式进行登记备案，确保其满足职责分离要求，填写《特权用户登记表》并负责归档。

- 网络管理负责人对网络管理员及其联系方式进行登记备案，填写《特权用户登记表》并负责归档。
- 特权用户发生变更和终止时，应及时更新《特权用户登记表》。

③ 管理员用户中，应用系统管理员不应兼任数据库管理员和操作系统管理员，应用系统管理员、数据库管理员和操作系统管理员不应参与本系统的日常业务交易处理，如会计凭证录入、凭证审批等。

（3）口令规则

1）初始口令规定

① 系统中的所有账号应有口令。

② 应用系统、数据库、操作系统、网络设备等系统的厂商初始口令应在系统投入使用前进行修改。

③ 系统管理员通过电子邮件告知用户本人其初始口令，并要求用户更改初始口令。

2）口令重置申请规定

① 当用户需重新申请口令时应提交《口令重置申请表》。

② 系统管理员审核《口令重置申请表》，帮助用户重新设置临时口令，通过电子邮件告知用户本人，并要求用户更改临时口令。

3）口令管理规定

① 普通用户口令的长度不应低于6位，特权用户口令的长度不应低于8位，如果系统能够实现口令长度的强制设定，则要求用户设置和修改口令应满足需求，如果系统不具备该功能，应通过电子邮件要求用户的口令长度应符合要求。

② 要求普通用户每隔90天至少修改一次口令，要求特权用户每隔30天至少修改一次口令，如果系统能够实现口令的强制定期修改，则要求用户在规定期限内修改口令；如果系统不具备该功能，应通过电子邮件要求

用户定期修改口令。

（4）用户权限管理

① IT 部门根据业务部门提供的职责分离表，转换成应用系统的职责分离矩阵。

② IT 部门将应用系统的职责分离矩阵提交给业务部门进行审阅和批准，并根据职责分离矩阵进行应用系统的用户权限设置。

③ 应用系统负责人在审批《用户账号及权限管理表》时，要根据用户岗位职责分配相应的用户权限。

（5）用户账号和用户权限定期审核制度

① 所有应用系统普通用户权限应每六个月审核一次，特权用户的权限应每三个月审核一次。

② 应用系统普通用户定期审核流程：

- 应用系统管理员每六个月将根据系统生成的当前普通用户清单及权限表提交给应用系统负责人。
- 应用系统负责人审核普通用户的权限分配是否符合岗位职责，并审核是否存在无人使用的账号，将审核结果填写在《应用系统权限检查表》中，并签字确认。
- 在应用系统负责人的监督下，应用系统管理员根据《应用系统权限检查表》，纠正不符的权限分配，并关闭无人使用的账号，并签字确认。
- 《应用系统权限检查表》及普通用户清单和权限表应抄报给本单位信息安全管理负责人，并由其负责归档。

③ 应用系统管理员、数据库管理员、操作系统管理员定期审核流程：

- 应用系统负责人每三个月审核应用系统管理员、数据库管理员和操

作系统管理员是否与《特权用户登记备案表》一致，其中，对应用系统管理员的审核结果填写在《应用系统权限检查表》中，对数据库管理员和操作系统管理员的审核结果填写在《操作系统/数据库权限检查表》中。

- 在应用系统负责人的监督下，应用系统管理员根据《应用系统权限检查表》，纠正不符的账号和权限分配，数据库管理员和操作系统管理员根据《操作系统/数据库权限检查表》，纠正不符的账号和权限分配。
- 《应用系统权限检查表》和《操作系统/数据库权限检查表》应抄报给本单位信息安全管理负责人，并由其负责归档。

④ 网络管理员定期审核流程：

- 网络管理负责人每三个月审核网络管理员是否与《特权用户登记备案表》一致，将审核结果填写在《防火墙系统权限检查表》中，并签字确认。
- 在网络管理负责人的监督下，网络管理员根据《防火墙系统权限检查表》，纠正不符的账号和权限分配。
- 《防火墙系统权限检查表》应抄报给本单位信息安全管理负责人，并由其负责归档。

（6）用户活动的监控

应用系统管理员每周检查应用系统日志，审查是否有错误信息或异常登录信息；网络管理员每周检查防火墙日志，审查是否有登录异常信息、配置更改。

（7）服务器操作系统设置规定

服务器操作系统的设置应符合公司的标准配置的要求。

① 服务器操作系统标准配置方案。公司 IT 部门负责编制服务器操作系统的标准配置方案。

② 服务器操作系统初始设置管理。各级下属公司的操作系统管理员根据公司的服务器操作系统标准配置方案进行设置，标准配置方案中未规定的内容保持原有设置。

③ 服务器操作系统设置变更管理。请参考变更管理的相关内容。

④ 服务器操作系统设置定期审核。信息安全管理负责人在操作系统管理员协助下，每年审核服务器操作系统设置是否符合标准配置方案，填写操作系统安全配置检查表并负责归档。

（8）数据的直接访问

当用户需要使用数据库专用工具对数据库进行直接数据访问时，应经过申请、审批后，由数据库管理员协助用户进行访问。

① 用户需要直接访问系统中的数据时，应填写《数据直接访问申请表》，说明访问申请原因和具体操作内容等。

② 《数据直接访问申请表》应由用户主管领导签字批准，提交应用系统负责人。

③ 应用系统负责人审批《数据直接访问申请表》，授权给数据库管理员进行操作。

④ 数据库管理员记录数据直接访问的对象和结果，如果存在数据修改，则须详细描述数据的修改步骤，并负责《数据直接访问申请表》的归档。

3．物理安全

（1）进入机房的物理安全访问控制机制

① 所有机房应使用门锁或电子门禁系统进行基础保护。

② 机房钥匙/门禁卡管理规定：

- 机房负责人负责机房钥匙或门禁卡的发放，将机房钥匙或门禁卡用户列入《进入机房授权人员名单》中，并负责《进入机房授权人员名单》的归档。
- 机房钥匙不应转借他人或复制，只有与卡号登记相符的用户才可以使用该门禁卡，各用户不应将门禁卡转借他人。
- 机房钥匙或门禁卡用户一旦发生离职或岗位变动等情况，机房负责人应及时回收钥匙，或调整、回收门禁卡，并更新《进入机房授权人员名单》。

③ 对于有值班人员控制进出的机房，机房负责人可将需要经常进入机房但没有机房钥匙或门禁卡的人员列入《进入机房授权人员名单》中。

（2）进入机房的登记管理

对于没有电子门禁的机房或门禁卡不能自动记录访问者账号、访问时间等信息的机房，应采取以下机房进入登记制度：

① 进入机房授权人员每次进入机房时，应按规定填写《机房出入登记表》后进入机房。

② 其他人员，包括内部临时进入机房人员和外部人员，须根据进入机房的事由，经进入机房授权人员同意后，按规定填写《机房出入登记表》进入机房。

③ 机房负责人负责《机房出入登记表》的归档。

（3）敏感的纸质系统文件管理

① 敏感的纸质系统文件应放置在带锁的文件柜里，包括与财务报表相关系统的设计、开发、测试、变更管理文档、用户使用手册，以及网络和基础设施的设计和变更文档等。

② 文件柜和纸质文件应由专门的保管人员进行管理，并由其负责纸质文件的借阅、使用和复制等处理活动记录的归档。

4. 网络安全

（1）网络设计、变更审批管理

① 公司IT部门负责制定网络的总体方案。

② 各级IT部门根据本下属公司的业务需要，结合公司网络总体方案，编制本单位的网络设计方案，并报公司IT部门审批、备案后实施。各级IT部门负责本单位网络拓朴图、IP分配表等网络设计文档的归档。

③ 网络变更管理。请参考变更管理的相关内容。

（2）边界网络设置管理

① 边界网络出口设置应与业务需求匹配：

- 各级IT部门对边界网络出口进行登记，填写《边界网络出口登记表》，详细描述与业务需求的匹配关系，并报公司IT部门审批。
- 各级IT部门需新增边界网络出口时，应填写《边界网络出口申请表》，报公司IT部门审批同意后执行，并由各级IT部门更新《边界网络出口登记表》。

② 防火墙配置管理：

- 防火墙安全配置标准。公司IT部门负责编制防火墙的安全配置标准。
- 防火墙初始配置。各级下属公司的网络管理员根据公司的防火墙安全配置标准进行设置，安全配置标准中未规定的内容保持原有设置。
- 防火墙配置变更管理。请参考变更管理的相关内容。
- 防火墙配置定期审核。信息安全管理负责人在网络管理员协助下，定期（每三个月）审核防火墙配置是否符合安全配置标准，填写《防

火墙安全配置检查表》并负责归档。

（3）网络监控与入侵检测

① 网络管理员每周检查防火墙日志，对网络进行监控，检测是否有非法入侵。

② 网络管理员应对监控软件和入侵检测系统发现的网络异常事件进行及时跟踪，并根据问题管理流程进行安全事件响应。

（4）远程登录管理

① 远程登录应通过安全可靠的方式进行，如 VPN。如果不能采用安全可靠的方式，如直接拨号登录，则应对传输的数据进行加密。

② 远程登录账号的申请和终止流程：

- 用户填写《远程登录账号申请表》，说明申请理由及登录时间期限，提交用户主管领导审批。
- 网络管理负责人审批《远程登录账号申请表》，确定用户权限。
- 网络管理员根据《远程登录账号申请表》进行网络设置，通知用户，并负责《远程登录账号申请表》的归档。
- 网络管理员应根据用户申请的期限，及时关闭到期的远程登录账号。

③ 远程登录账号检查流程：

- 网络管理员每三个月将远程登录账号清单提交给相关网络管理负责人。
- 网络管理负责人审核用户远程登录账号是否合理，以及是否存在无人使用的用户账号，将审核结果填写在《远程登录权限检查表》中，并签字确认。
- 在网络管理负责人的监督下，网络管理员根据审查结果，关闭不合理和无人使用的远程登录用户账号，并签字确认。

- 远程登录权限审查结果应抄报给本单位信息安全管理负责人，并由其负责归档。

④ 远程登录应通过系统登录验证机制实现，应满足系统登录验证机制的要求。

5. 计算机病毒防护

（1）防毒软件安装范围

① 用户应了解未经授权或恶意软件的危险性，采取必要措施，包括通过安装防病毒软件等来防止和探测恶意软件进入系统。

② 安装 Windows 操作系统的服务器和个人计算机，要求安装统一的防病毒软件。

（2）病毒库更新

① 应及时更新防病毒软件商发布的最新病毒库。

② 如果有突发性的恶性病毒发生，网络管理员应通过电子邮件或门户网站发布病毒更新通知及处理办法，员工应及时参照执行。

（3）定期扫描

防病毒软件应打开定期扫描和实时监控功能，至少设置为每月扫描，员工不应采取任何方式（如关闭实时监控程序、卸载程序等）将防病毒软件设置成无效状态。

6. 第三方安全管理

（1）第三方供应商服务合同中有关信息安全的必要条款及监督

与第三方供应商达成的合同或协议应明确阐述公司的信息安全规定和要求。如果合同或协议涉及其他方，授权第三方访问的协议须包含其他方

的访问授权和访问条件。

合同执行部门应对第三方在合同执行过程中的安全行为按照合同的要求进行监督。

（2）第三方供应商对应用系统访问的管理措施

① 第三方需要访问公司应用系统生产环境时，应填写《用户账号及权限管理表》，说明账号使用的时间和期限，并得到相关业务部门主管领导的批准。

② 应用系统负责人审阅《用户账号及权限管理表》，确保其权限分配符合职责分离的要求，并签字确认。

③ 应用系统管理员负责在系统中创建用户，通知用户，并负责《用户账号及权限管理表》的归档。

④ 访问结束或访问期限到期，应用系统管理员应及时收回相应的访问权限。

（3）第三方供应商对系统远程登录的规定

① 第三方供应商如需要远程登录公司内部网络，应事先提出申请，填写《远程登录账号申请表》。

②《远程登录账号申请表》应由相关负责人员审批。

③ 网络管理员根据审批的结果赋予用户账号。

④ 访问结束或期限已到时，网络管理员应及时收回相应的远程登录权限。

7. 信息安全事件响应

信息安全事件应依据其对业务的影响程度和安全损害的严重程度，根据问题管理流程进行信息安全事件响应。

4.3.3 项目建设管理

1. 项目立项

（1）项目立项审批

① 项目建设单位根据自身业务需求，向本单位 IT 部门和规划计划部门提出开发项目立项申请。

② 立项申请经审批同意后，项目建设单位开始进行可行性研究。可行性分析报告应包括以下基本要求：项目目标与范围、现状与需求分析、技术方案、系统设计、组织机构与定员、实施计划、实施投资估算、实施风险与效益分析。

③ 项目可行性研究报告完成后，提交本单位 IT 部门和规划计划部门审批，最终确认项目是否立项。

（2）商业软件及硬件的外购

对已经通过立项审批和可行性研究且需要进行商业软件、硬件及服务外购的项目，在项目立项审批通过后，按照采购流程进行商业软件、硬件及服务的外购，如果需要进行招投标，按照招投标流程执行。

2. 项目建设方法论

项目的建设应按生命周期法分阶段进行，包括项目启动、项目需求分析、项目设计、系统开发实施、系统测试、数据移植、系统上线、项目验收和上线后评估。

（1）项目启动

项目启动后，成立项目指导委员会，当项目有多个子项目时，可成立项目管理办公室，任命项目经理，并确定项目的组织结构和成员，其中，

所有业务应用系统实施项目的项目组都应包括业务部门的相关负责人。项目经理应组织制定项目的总体计划，内容包括：

1）项目范围

项目范围描述对项目范围如何进行管理，以及项目范围怎样变化才能与项目要求相一致等问题，用以衡量一个项目或项目阶段是否已经顺利完成。

2）项目进度管理

项目进度管理描述如何对项目进度的变更进行管理，用以保证项目在期望的时间内完成。

3）项目人员需求

项目人员需求描述项目的组织结构及其中各个岗位职责，用以明确各个项目成员在项目中的责任和义务。

4）项目沟通管理

项目沟通管理描述项目团队如何创建、收集、发送、储存和处理项目相关信息等内容，用以保证满足项目相关利益方在项目沟通方面的需求。

根据项目需要，项目总体计划也可以包括下列补充内容：

① 项目成本管理。项目成本管理描述当实际成本与计划成本发生偏差时如何进行管理，用以保证项目在批准的预算范围内完成。

② 项目质量管理。项目质量管理描述项目团队如何具体执行质量政策，为项目提出质量控制、质量保证和质量提高方面的措施，确保项目实现其质量目标。

③ 项目风险管理。项目风险管理计划描述在项目整个生命周期中，风险识别、风险定性和定量分析、风险应对计划、风险跟踪和控制是如何建

立和执行，用以管理整个项目过程中所出现的风险，以规避或减轻风险对项目的不利影响。

④ 项目培训。项目培训描述项目的有关培训活动，包括培训时间、地点、参加人员、所需资源、培训考核方法等。

项目总体计划各项内容制定完毕后，交项目管理办公室和项目指导委员会进行审批，并由项目经理负责审批后总体计划的归档。

（2）项目需求分析

需求分析工作的主要任务就是对项目实施各相关方面的现状及各级用户的具体需求进行调研和分析，最终形成需求分析报告。

1）设计现状、需求调研和访谈问卷

项目经理组织各项目小组设计各组分管的现状及需求方面的访谈问卷，收集各组分管的项目相关方面的现状及各类需求。在各小组完成问卷设计后，项目经理需要对内容进行审阅，并组织各组与相关业务部门主管领导及成员就问卷内容进行讨论，最终定稿。

2）确定访谈方式和范围

项目经理组织项目成员共同讨论，确定调研访谈对象及方式，制定调研和访谈计划。

3）按访谈计划安排并进行调研和访谈

访谈各项准备工作完成后，项目组成员依据访谈计划，开始调研和访谈。

4）收集整理访谈资料

访谈之后，各项目小组汇总整理各自的访谈纪要，并收集整理下发的问卷。

5）编制需求报告

根据调研、访谈及其他途径收集来的信息，项目经理组织各项目小组进行各分管方面的现状及需求的分析，并编制需求分析报告，内容包括：

① 基本要求。项目的目标、背景；业务需求描述。

② 可选要求。组织结构和业务部门设置；业务现状；信息系统现状；组织和业务的未来发展计划；项目的性能期望，如预期用户数、在线用户数、关键操作的响应速度等；项目的前身及与相关系统的联系；项目的界面要求。

6）需求分析报告完成后，项目经理与相关业务部门主管领导就需求分析报告进行讨论和确认。业务部门主管领导应在文档上签字确认。

（3）项目设计

项目设计就是根据选定的系统，在前一阶段需求分析的基础上，对系统实施的所有细节，包括业务流程、应用架构、技术架构和数据架构等做进一步的确定和细化设计，形成系统设计说明书，内容包括功能实现、系统安全等方面的设计。

项目设计应包括以下主要流程和工作内容：

1）概要设计

结合需求分析报告及行业最佳实践，进行系统概要设计，内容涵盖应用架构、技术架构和数据架构等方面。

2）成立数据收集小组

如果项目实施涉及数据收集，应成立数据收集小组，确定数据收集计划，设计数据收集格式及表格，并开始进行数据收集。小组成员包括关键用户和系统各主要模块的实施人员。

3）进行业务流程设计

结合系统功能和用户实际需求，对业务流程进行详细设计，设计应反

映内部控制关键点。业务流程的设计，应有统一的流程图制作规范和相应的说明，企业核心业务流程应给出明确定义和重点说明。

4）编制设计说明书

由项目经理负责组织开发团队成员编制设计说明书。设计说明书内容包括：

① 基本要求。业务详细需求，包括业务描述、业务流程、内部控制关键点等；功能说明，包括功能描述、主要功能模块组成和相互关系；项目运行的软硬件平台及对客户端软硬件环境的特殊要求。

② 可选要求。相关模块间的接口，即模块间传递信息的内容、方式和协议；确定各模块在计算机网络环境下的物理分布；确定本系统与其他外围系统接口；用户界面的设计风格；主要算法设计；异常处理设计；安全性设计说明。

5）与相关方讨论、确认签字

项目经理与相关业务部门主管领导就设计说明书进行讨论和确认。业务部门主管领导应在文档上签字确认。

（4）系统开发实施

① 对于有编程开发需求的系统项目，开发小组应首先建立编程标准，该标准包括但不限于命名规则、注释规则、格式规则。全体开发人员执行该标准，根据设计说明书进行编程工作，程序文件的注释要做到清晰、详尽，便于将来的查阅和修改。

② 在进行系统配置的时候，项目成员应对各项功能设置的步骤、参数等都进行详细的记录，形成系统配置文档。最终的系统配置文档是经过反复修改调整后形成的，在每次进行或调整系统配置时，都应更新相应的系统配置文档。

③ 客户化工作是根据用户需求，在现有系统的基础上，对需要进行自行开发的部分进行客户化编程。当需要进行客户化程序开发时，开发人员根据设计说明书中的客户化功能说明，进行编程工作。客户化工作阶段可与系统配置阶段同时进行。

④ 开发和实施人员不应访问生产环境，开发工作应在开发环境中进行。

（5）系统测试

系统测试是对系统进行全面的测试，应在测试环境中进行，以确保系统的功能和技术设计满足企业的业务需求，并正常运行。

系统测试阶段应包括以下主要流程和工作内容：

1）制定测试计划，编制测试用例，建立测试环境

项目组制定详细的测试计划，编制相应的测试用例，并根据测试用例及相关的标准建立测试环境。测试内容要关注与内部控制相关的系统安全访问、系统接口、数据输入/输出和数据完整性等关键控制点；测试环境根据测试计划及相关的标准建立，测试环境和生产环境应进行隔离。测试计划内容包括：

① 基本要求。测试目的、测试范围；测试环境，包括服务器和客户端所需的硬件、软件等；测试安排，包括测试时间、测试内容、测试步骤、预期测试结果。

② 可选要求。测试参与人员、测试方法。

2）测试

在测试环境中，项目组根据需要，对系统依次进行单元测试、集成测试、压力测试和用户接受测试，记录测试结果并由相关测试人签字确认，编制相应的测试报告。对于未通过测试的内容，项目组应查找失败的原因，

并修改相应程序或设置，重新进行测试。除了进行充分的系统功能测试，测试应包含与内部控制相关的测试内容，如系统认证和授权、交易完整性及数据真实、完整性的有关功能。

① 单元测试是对系统的各个相关模块功能进行整合测试，以检查数据在不同功能中的流通/传递是否正确，各个模块功能有无相互抵触。

② 集成测试是针对包含多个子系统、应将各子系统结合起来进行的测试。

③ 压力测试是模拟将来实际工作中可能出现的瓶颈/极限条件，对系统进行压力测试，测试系统的反应情况。

④ 用户接受测试是关键用户对系统进行的测试，用户应对测试结果签字确认。

3）提交测试报告、用户确认签字

项目组撰写测试报告，将测试报告提交给各相关用户，用户应在测试报告上签字确认。测试报告内容包括：

① 基本要求。测试目标；测试结果，包括测试内容、测试步骤、预期测试结果、实际测试结果，测试人；测试结果分析。

② 可选要求。测试人员组成；测试方法；测试工作的组织方式；测试工作的计划安排。

- 项目组将测试后的系统源代码交专人保管。
- 系统测试阶段结束后应归档的文档包括测试计划、测试用例、测试报告。

（6）数据移植

新系统上线时如需要将原始数据移植到新系统，则应完成以下主要工作内容：

1）制定数据移植/转换计划

该计划中除了要定义数据收集的格式、范围、进度外，还要考虑系统接口的影响，并建立数据移植完整性和准确性测试方法及意外事件处理程序。

2）数据收集

如果项目实施涉及数据收集，应由数据收集小组根据数据收集格式，对数据进行收集，数据收集小组在收集数据时应培训业务部门的数据提供人员，以确保数据提供人员了解和掌握对数据收集的各项规定和要求。

3）将收集到的数据存放于指定目录下，由专人管理

4）进行数据清理

5）测试数据移植方法

数据移植前，在测试环境中对数据移植方法进行测试，书面记录测试结果，解决测试中发现的问题，进行问题记录并归档。

6）数据导入并核查结果

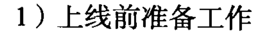
项目组成员将数据导入系统，并在导入后按照事先制定的数据移植完整性和准确性测试方法对系统中的数据做进一步的核查，确保导入数据的质量。如有意外，按照事先制定的意外事件处理程序处理，并留下记录。数据移植完成之后，用户应对数据移植结果签字确认。

7）试运行

数据移植后要进行适当时间的试运行，确认数据移植的真实性和完整性。试运行时间视具体系统的规模、影响程度而定。对影响较大的系统，至少应试运行三个完整的月结周期。

（7）系统上线

系统上线阶段应包括以下的主要流程和工作内容：



1）上线前准备工作

① 在上线前，项目经理要组织项目组制定系统上线计划，包括上线检查清单、上线支持人员、退回机制等，并提交《上线申请表》。

② 系统上线计划和《上线申请表》应经过 IT 部门和业务部门管理层的正式批准，并通知各相关部门。

③ 程序保管人员根据审批后的《上线申请表》，将通过测试验收的最后版本的系统程序提交系统上线操作人员。

2）系统上线

① 所有的上线准备工作做好之后，由项目建设单位提前通知用户系统上线时间，项目经理在确认上线系统版本正确性后，下达上线指令。

② 系统上线操作人员负责将最后版本的系统程序移植到生产环境。

（8）项目验收和上线后评估

1）项目验收

项目验收是指项目进行到某一阶段或项目结束时，项目组将其成果交付之前，由各相关部门，包括 IT 部门、项目建设单位、实施方等，对项目的成果进行验收。项目验收情况应经过验收各方的签字确认。

2）上线后评估

在项目建设完毕投入使用一个月后，由项目建设单位组织成立评估小组，开展上线后评估工作，并出具评估意见，对于发现的问题，应提交项目建设单位及时解决。项目建设单位负责上线后评估相关文档的归档。

3．项目管理

（1）项目培训管理

1）培训对象

用户培训主要是针对三类人群：系统支持人员、系统关键用户和一般

用户。

① 系统支持人员。主要负责系统配置维护及用户管理，由软件供应商或项目组进行培训。

② 关键用户。一般为业务骨干，处于业务流程关键岗位，熟悉业务流程，由软件供应商或项目组进行培训。

③ 一般用户。系统上线后进行日常工作的普通用户，可以由关键用户对其进行培训，也可以由软件供应商或项目组进行培训。

2）培训实施过程

① 项目经理在项目启动阶段，就应组织项目组成员针对三类不同用户制定相应的培训计划。

② 项目组编写各类使用人员的培训材料、使用手册，包括各个模块的操作步骤说明、操作界面等，并负责各种文档的归档。

③ 对系统支持人员、关键用户和一般用户分别组织培训。

（2）项目文档管理

1）项目文档的分类

项目文档分为系统开发文档和项目管理文档。

① 系统开发文档包括可行性分析报告、需求分析报告、设计说明书、测试计划、测试报告、数据移植文档及用户手册。

② 项目管理文档包括项目总体计划、项目会议纪要、项目阶段报告等文档。

2）用户手册和培训材料的编写

用户手册和培训材料的编写应详细、实用，并且应随着系统的更新进行版本更新。

3）项目文档的保管

在项目过程中，项目负责人或由其指派专人负责项目文档的保管，在

项目验收后，项目建设单位或 IT 部门负责项目文档的归档。

4）开发文档的保存

开发文档在系统的使用期内妥善保存，可以以电子或纸质形式存在，并应按照项目规定的规则命名。电子文档应存放在项目约定的文件服务器的文件夹或存储介质中。

5）项目文档的控制

项目文档应有版本控制措施，如编写文档版本号、更新时间等。

（3）项目沟通管理

① 项目组应在项目开始时制定完善的项目汇报制度，明确沟通时间、频率和渠道。

② 项目组在项目过程中应定期就该项目根据生命周期方法论的执行情况向项目指导委员会汇报。

（4）项目变更管理

① 项目进程中，项目组发现变更需求后，应填写变更申请单，上报项目经理。

② 项目经理审查分析变更对项目的影响：

- 属于项目经理职责范围内，由项目经理决定是否变更。
- 超出项目经理职责范围的变更请求，项目经理应上报项目管理办公室负责人，确定是否变更。如同意变更，项目管理办公室负责人要审批签字，下达项目经理执行。
- 如变更请求超出项目管理办公室的职权范围，应上报项目指导委员会，由委员会讨论、决策。委员会领导签字审批后下达项目管理办公室，由项目管理办公室下达项目经理执行。项目组应对变更进行备案。

③ 项目组执行变更。

④ 实施变更后，项目组要更新变更过程文档并负责归档。

（5）项目问题管理

① 项目进程中发现问题后，应上报项目经理，由项目经理组织设计解决方案。

② 项目经理与项目组成员沟通后实施解决方案：

- 如问题不能在项目组范围内解决，项目经理应把问题上报到项目管理办公室，由该办公室负责分析问题并设计解决方案，与项目经理沟通后由项目经理执行，项目经理应对问题进行跟踪记录，并负责问题记录文档的归档。
- 如项目管理办公室也无法解决问题，办公室应上报项目指导委员会，由委员会讨论做出决策，然后通知项目管理办公室，由其执行，项目管理办公室应对问题进行跟踪记录，并负责问题记录文档的归档。

（6）环境隔离

① 在项目的执行过程中，应确保开发、测试和生产环境的隔离。

② 项目经理应对项目执行过程中是否符合环境隔离要求进行审阅，并将审阅结果反映在项目阶段报告中。

4.3.4 系统变更管理

1. 变更管理

（1）系统变更的定义

系统变更包括对应用系统的升级、修改、补丁安装等改变系统功能的活动，以及对操作系统升级和补丁安装、数据库/操作系统环境配置变化、防火墙配置修改等。

（2）变更申请的跟踪

IT 部门负责人应指定专门人员每月检查所有系统变更申请的执行情况，填写《变更统计表》，并提交给 IT 部门负责人审阅，确保审批过的变更被及时执行，并及时了解变更进度。IT 部门负责《变更统计表》的归档。

（3）变更的优先级别

根据变更对业务的影响程度，在提出变更申请时应定义该变更活动的优先级，分为以下三级：

① 高。如果变更不能尽快完成，将会对业务产生严重影响，并且没有替代措施可以降低该影响。

② 中。如果变更不能尽快完成，将会对业务产生一定影响，但受到影响的业务重要性不高或有临时替代措施可以降低影响。

③ 低。变更对业务影响不大，或有替代措施可以基本消除该影响。

（4）未授权变更活动的管理

禁止一切在未经授权的情况下对系统进行变更的行为，IT 部门对生产环境中未经授权的变更进行监测。

2. 日常变更流程

系统变更包括对应用系统的升级、修改、补丁安装等改变系统功能的活动，以及对操作系统升级和补丁安装、数据库/操作系统环境配置变化、防火墙配置修改等。

应用系统的升级、修改、补丁安装等变更活动由应用系统负责人进行审批；对操作系统升级和补丁安装、数据库/操作系统环境配置变化、防火墙配置修改等变更活动由 IT 部门负责人进行审批。

（1）变更申请与受理

① 用户申请变更时应填写《变更申请表》，确定变更类型，说明变更

原因、内容变更预期时间等内容后，将《变更申请表》提交主管领导。

② 主管领导审批《变更申请表》后，提交相应的应用系统负责人（或IT部门负责人）。

③ 应用系统负责人（或IT部门负责人）审批《变更申请表》后，确定变更的优先级，判断是否需要测试，并负责归档。

（2）变更实施

① 负责变更实施的IT人员填写《变更实施表》相关内容，并判断是否需要进行源代码修改。如果不需要，进行下一步操作；如果需要，填写《源代码变更交接表》，在应用系统负责人批准后，从系统源代码保管人处取得所需的系统源代码。

② 负责变更实施的IT人员在《变更实施表》中提出解决方案，内容包括实施步骤、回退机制，并在实施完成后记录实施结果。

③ 负责变更实施的IT人员建立与生产环境相隔离的开发环境，并在其中进行变更实施。

（3）变更测试

① 如果需要测试，负责变更测试的IT人员在《变更实施表》中提出测试计划（包括测试内容、步骤等），编制相应的测试文档，并根据测试文档及相关的标准建立测试环境。测试环境应与生产环境隔离。

② 负责变更测试的IT人员对变更的系统进行相关测试，记录测试结果，并签字确认。

③ 通过测试后，将最后版本的程序交专人保管，双方签字确认，防止任何未授权的更改。

（4）变更上线

① 变更申请人的主管领导、应用系统负责人（或IT部门负责人）应

共同审核是否可以上线。

② 负责变更实施的IT人员提前通知用户变更的上线时间。

③ 源代码保管人使用正确的版本进行系统上线。

（5）变更文档管理与培训

① 系统、用户及控制文档应及时更新。在变更过程中，上述文档由该变更活动的负责人或由其指派专人负责保管，在变更结束后，由应用系统负责人（或IT部门负责人）指定专人负责归档。

② 如果系统的变更导致用户操作的改变，应对用户进行培训，确保业务活动在系统变更后不受影响。

3．紧急变更流程

紧急变更是指由于突发事件且情况紧急，如果不立即采取措施，按照正常变更管理流程，将会严重影响正常业务运作的变更。

当发生紧急变更时，相关人员应立即通知其主管领导、应用系统负责人（或IT部门负责人），在获得批准后，可立即采取变更措施。但事后应补填《变更申请表》、《变更实施表》等相关表单。

4.3.5 信息系统日常运作

1．机房环境控制

（1）机房设址及建筑结构方面的基本要求

计算机机房不同于其他办公房间，技术要求较高、投资较大。因此，在建立计算机机房时，应依据计算机系统的规模、用途、任务、性质的不同而设置。

计算机机房场地的环境选择和建筑设计应按国家相关规范的要求执行。

（2）机房环境控制设备的要求

机房环境控制的具体要求如下：

1）布线

① 计算机机房应合理布线。电源可采用地下电缆进线，并采取避雷措施；当采用架空进线时，应在低压架空电源进线处或专用电力变压器低压配电母线处装设低压避雷器。

② 电源线应尽可能远离计算机信号线，并避免并排敷设。

2）温度及湿度

① 机房内应配备独立电源空调。

② 机房内应配备温度、湿度计，机房的温度、湿度应保证内部设备正常运行。

3）消防报警

① 机房应配备消防设施，并按消防部门的要求，定期检查其有效性。消防设施应尽量放置在过道等明显的位置。

② 在机房内应设置烟雾探测器。

4）防静电及防雷接地

① 机房应使用防静电地板。

② 机房应按照国家规范，安装防雷接地设施。

5）不间断电源系统

① 机房内的关键设备应采用不间断电源系统（UPS）供电。

② UPS 设备及其电池组应按产品说明书的要求定期进行检查和维护。

2. 系统日常运作监控

① 机房负责人应指定人员每天对设备运行状况进行巡检，检查内容包括设备电源、风扇、指示灯、报警信息、机房温度及湿度等，检查人员

填写《设备巡检记录表》，签字确认并负责归档。

② 应用系统管理员应每周检查应用系统日志，审查是否有错误信息或异常登录信息等，填写《应用系统日志检查记录表》，签字确认并负责归档。

③ 网络管理员应每周检查防火墙日志，审查是否有登录异常信息、配置更改、功能停止、会话连接异常等，填写《防火墙日志检查记录表》，签字确认并负责归档。

3. 批处理作业调度管理

（1）批处理作业调度管理流程

① 应用系统管理员应根据业务需求，编制《批处理作业清单》及《批处理作业详细说明书》。

② 《批处理作业详细说明书》由应用系统负责人基于业务需求进行审核，经批准后遵照执行。应用系统管理员负责《批处理作业清单》及《批处理作业详细说明书》的归档。

（2）批处理作业变更管理

当需要进行批处理作业变更时，由应用系统管理员重新编写《批处理作业详细说明书》，并更新《批处理作业清单》，提交给应用系统负责人进行审核，经批准后遵照执行。应用系统管理员负责《批处理作业清单》及《批处理作业详细说明书》的归档。

（3）批处理作业的监控

应用系统管理员根据具体批处理作业的检查周期，定期检查批处理作业的执行情况，填写《批处理作业记录表》，签字确认并负责归档。

4．备份与恢复

① 应用系统负责人应指定人员根据应用系统的重要程度，制定备份和恢复策略，填写《备份作业清单》及《备份作业详细说明书》，并经过应用系统负责人审批。应用系统负责人每年审阅《备份作业清单》及《备份作业详细说明书》，如果其已经不能满足业务需求，应指定人员进行调整。应用系统负责人负责《备份作业清单》及《备份作业详细说明书》的归档。

② 备份和恢复策略主要包括备份数据内容、备份方式、备份频率、操作方法、备份及恢复操作步骤、备份介质存放地点等。

③ 应用系统负责人应指定人员依据《备份作业清单》及《备份作业详细说明书》，执行备份操作，填写《备份记录表》，离线备份存储介质应进行适当的安全保护。

④ 备份恢复测试。应用系统负责人指定人员每年，或备份方法、步骤或环境发生重大变化时，进行恢复性测试，以确保数据能够准确及完整地恢复，测试人员应将测试过程及结果记录在《备份恢复测试记录表》中，应用系统负责人签字确认并负责归档。

⑤ 备份恢复：

- 当由于业务需要或系统故障等情况需要进行备份恢复时，业务用户填写《备份恢复管理表》，说明备份恢复原因，提交其主管领导审批。
- 业务用户主管领导审批通过后，提交应用系统负责人，由应用系统负责人指定人员制定详细的恢复步骤，并填写《备份恢复管理表》中的相关内容，由应用系统负责人审批通过后执行。
- 业务用户主管领导对备份恢复的结果进行确认签字。
- 应用系统负责人负责《备份恢复管理表》的归档。

5. 问题管理

（1）问题管理流程

① 建立问题管理机制，由专职或兼职的帮助热线支持人员受理各类信息系统及其相关设备发生的问题，负责问题的记录与解答。帮助热线支持人员可为信息系统技术人员（如应用系统管理员），也可为其他员工。

② IT 部门将各帮助热线支持人员的名单和联系电话及其所负责处理的问题类型登记在《信息系统故障处理帮助热线支持人员联系表》中，并发布给所有员工。联系表上的帮助热线支持人员发生变动时，IT 部门应及时更新。

③ 发生问题时，用户在《信息系统故障处理帮助热线支持人员联系表》中找到负责处理相应问题的帮助热线支持人员，通过邮件、电话或口头提交问题。

④ 帮助热线支持人员接到问题报告时，应及时在《问题记录日志表》中进行记录，记录内容包括汇报人、所属部门、问题类型和问题描述等。

⑤ 如果帮助热线支持人员由信息系统技术人员兼任，可根据问题类型直接解决该问题，否则应将《问题记录日志表》提交给相关技术支持人员对问题进行处理。

- 相关技术支持人员解决问题后，在《问题记录日志表》中注明问题原因、解决方法和解决时间，并签字确认，将该表返还帮助热线支持人员，帮助热线支持人员确认问题解决后，在该表上签字后并负责归档。
- 帮助热线支持人员应定期分类汇总当月发生的问题，形成书面分析报告《问题分类汇总月报表》，向本部门主管领导汇报，并负责归档。

（2）问题重要程度分级

按照问题的影响程度，IT 问题可分为高、中、低三个级别。

① 高。影响到大多数用户工作的问题，如系统崩溃、网络瘫痪和全局性安全问题；虽然影响到部分用户，但是严重影响财务部门进行账务处理的问题，如财务管理信息系统某个子模块发生问题。

② 中。影响到部分用户工作的问题，如库存管理系统发生故障影响到物资管理部门的工作，或发生在部分用户的系统非法入侵和病毒攻击等。

③ 低。影响到个别用户工作的问题，如个人计算机硬件故障和办公软件安装等。

（3）问题汇报

根据问题的重要程度上报至相关部门负责人，进行汇报。

① 高级别问题。高级别问题应在问题确认后一天内，由相关帮助热线支持人员以书面形式向本部门主管领导汇报，同时抄报本单位信息安全管理负责人，并由信息安全管理负责人以书面形式上报至上级单位信息安全管理负责人。上级单位信息安全管理负责人负责高级别问题书面汇报的归档。

② 中级别问题。中级别问题确认后，相关帮助热线支持人员应在五个工作日内以书面形式向本部门主管领导汇报，同时抄报本单位信息安全管理负责人。本单位信息安全管理负责人负责中级别问题书面汇报的归档。

③ 低级别问题。相关帮助热线支持人员每月通过《问题分类汇总月报表》，向本部门主管领导提供包括低级别问题在内的情况汇报。

4.3.6 最终用户操作

1．最终用户计算机操作安全制度

① 员工不应采取不正当手段获取商业秘密，更不应未经本公司许可，

披露或者泄露本公司的商业秘密。

② 员工对所使用的信息和软硬件负有安全责任。员工有责任及时发现并上报发生的信息安全事件，并应在信息安全事件的处理过程中协助相关人员的调查、处理工作。

③ 员工有责任管理好各种用于身份认证的账号、口令、门卡等，不应使用他人账号，也不应与他人共享。口令的设置和使用应符合口令规则。

2. 电子表格管理

（1）电子表格控制策略

① 与财务报表相关的电子表格纳入电子表格管理范围，依据其用途和复杂程度，分为重要电子表格和一般电子表格。

- 重要电子表格。作为财务报表或财务账户的直接或间接数据来源，通常包含比较复杂的运算或多重表格关联。
- 一般电子表格。不影响财务报表或财务账户，但是用于评估财务数据的真实性、完整性和准确性。

② 各业务部门在《电子表格登记表》中登记纳入管理范围的与财务报表相关的电子表格。《电子表格登记表》应包含电子表格名称、版本、负责人、用户、开发人，以及电子表格内容概要和影响的财务科目，并在纳入管理范围的电子表格开发或变更完成后，由电子表格负责人及时更新《电子表格登记表》。

③ 对于纳入管理范围的电子表格，要根据其分类，建立相应的控制级别。在安全、版本、变更、开发、备份和存档等方面，重要电子表格应实施严格的控制措施。即使是一般电子表格，也应对安全、版本和变更进行控制。

（2）安全控制

重要和一般电子表格的日常使用应遵循以下原则。

① 授权。用户使用电子表格应得到相应的批准审核，具体可分为两类情况：

- 新员工到职时，其主管领导根据岗位职责，将其工作所需的电子表格授权给该员工。
- 如果因工作原因，需要使用到职时获得授权以外的电子表格，应向主管领导提交《电子表格使用申请表》，主管领导依据工作需要审批《电子表格使用申请表》，审批通过后，该员工才能使用。主管领导负责《电子表格使用申请表》的归档。

② 存储路径保护。电子表格负责人应将电子表格存放在文件服务器受到保护的路径目录下，并对电子表格存放目录权限进行控制。

③ 文件访问控制。电子表格负责人应确保电子表格已设定口令保护，只有得到授权的用户才能使用该电子表格。

④ 文件内容保护。电子表格负责人应采取必要措施，确保只有经授权的人员才能更改电子表格中的预设公式和数值等内容。

（3）版本控制

① 重要和一般电子表格应遵循命名规则，电子表格模板文件的文件名要体现版本号，电子表格数据文件的文件名要体现最后保存日期。

② 重要和一般电子表格的版本管理由电子表格负责人负责，电子表格进行变更后，电子表格负责人要通过电子邮件等方式，通知该电子表格用户及时使用最新版本的电子表格。

（4）变更管理

重要和一般电子表格的变更应严格遵循电子表格变更管理的规定，包

括申请、授权、测试和批准的完整过程。电子表格负责人负责该过程文档记录的归档。

① 申请。当需要进行电子表格变更时，用户应填写《电子表格变更申请表》，说明其变更申请和变更原因等内容。

② 授权。电子表格负责人依据业务需要批准《电子表格变更申请表》后，开发人员才有权对电子表格进行变更。

③ 变更开发与测试。开发人员根据《电子表格变更申请表》进行变更开发，电子表格的变更文档要说明该电子表格的变更设计细节，如电子表格中公式的设定方法，同时编写或更新相应的用户操作说明。变更开发后应进行测试，测试结果要经用户签字确认。

④ 批准。测试完成后，电子表格负责人要对测试结果进行审阅并签字确认，之后，将经过变更的电子表格重新投入使用，同时更新《电子表格登记表》。

（5）开发管理

重要电子表格的开发应严格遵循电子表格开发管理的规定，包括申请、授权、测试和批准的完整过程。电子表格负责人负责该过程文档记录的归档。

① 申请。当需要进行电子表格开发时，用户应填写《电子表格开发申请表》，说明其开发申请和开发原因等内容。

② 授权。业务部门主管领导依据业务需要批准《电子表格开发申请表》后，开发人员才有权对电子表格进行开发。

③ 开发与测试。开发人员根据《电子表格开发申请表》进行开发，电子表格的开发文档要说明该电子表格的设计细节，如电子表格中公式的设定方法，同时编写相应的用户操作说明。对重要电子表格进行开发后，应

进行测试，测试结果要经用户签字确认。

④ 批准。测试完成后，指定电子表格负责人，由其审阅测试结果并签字确认，之后，将开发的电子表格投入使用，同时更新《电子表格登记表》。

（6）备份管理

重要电子表格应定期备份，确保数据的完整性与准确性。重要电子表格的备份分为两类：

① 电子表格模板的备份。电子表格模板的备份由电子表格负责人指派相关人员负责，存放在文件服务器指定的文件夹中。

② 电子表格数据的备份。电子表格的数据备份由用户各自进行，根据使用的频率决定备份的周期。

（7）存档管理

电子表格负责人应指定相关人员，每年对重要电子表格进行存档，将其存入独立的存储介质，并设置为只读模式。

4.4 业务层面内部控制建设

4.4.1 业务流程梳理

1. 概念

业务流程梳理，就是将企业各项业务活动、相关要素及其关联性以业务流程的形式反映出来的活动。它的基本内涵有以下几个方面：

① 业务流程梳理的内容是具有关联性的企业各项业务活动，凡是纳入一个业务流程的业务活动均具有内在的关联性，这些活动可以是某一部门内部的，也可以是跨部门的。

② 业务流程梳理的形式一般采取访谈的形式，即由专业流程管理人员对实际岗位操作人员进行访谈，了解流程的基本内容，经过整理和反复确认，形成相对固化的业务流程。

③ 业务流程梳理的结果是形成一整套固化的业务流程体系。

第3章已经基本识别出了与财务报告相关的业务流程体系。

2. 业务流程梳理的意义

（1）是规范工作秩序的前提

可以将各项业务活动与岗位设置、岗位职责、工作制度等诸因素结合起来，形成了一整套有着内在有机联系的工作程序：为什么设置这个岗位，这个岗位应该从事哪些工作，依据的制度是什么，形成哪些证据等，都一目了然、非常清楚，有利于规范工作秩序。

（2）是识别风险的前提

风险存在于企业经营活动的各个方面，但是如果离开了业务流程，风险将无法捕捉，也就无法控制。概括地说，风险存在于具体的业务流程当中，业务流程是识别风险的具体载体。我们可以顺着业务流程的脉络梳理风险，设置控制措施。

（3）分析控制措施及分析风险管理水平的前提

对于风险的管理和控制要依托流程梳理来完成。分析控制措施及分析风险管理水平首先要看流程梳理的水平，如果我们梳理出来的流程无法实现对风险的有效控制和管理，说明我们的流程梳理工作需要进一步改进和完善。因此我们分析一家企业对于风险的控制措施是否完善，对于风险的管理到底有多高的水平，很重要的一个方面是要看它的流程梳理工作是否完善。

（4）是进行流程管理、内部控制建设及 ERP 建设的前提

毫无疑问，流程梳理及梳理工作的成果将成为流程管理的主要内容，是做好企业内部控制建设的前提，也为即将要上的 ERP 奠定基础。

3．业务流程梳理内容

业务流程梳理的内容就是对企事业单位主要流程中的末级流程，从始点到终点，理清发生在实际业务中的步骤节点，执行的部门岗位，流转的文件及记录表单，风险可能产生的环节，存在的控制，对该业务起到规范性要求的文件及规章制度等。

业务流程梳理贯穿风险控制分析的全过程，通过不断梳理，完成对流程的描述和风险控制矩阵的编制，并不断使之完善。

4．业务流程梳理程序及方法

（1）确认部门、岗位名称

流程梳理涉及部门、岗位的名称，确保同一部门、岗位名称在不同流程中使用的一致性，并与实际一致。

（2）业务流程梳理的步骤

第一步　针对要梳理的业务流程，明确该流程的起点和终点，分别向该业务流程涉及的岗位人员进行访谈，主要了解什么岗位在什么情况下做了什么并形成哪些文档或表格等，详细掌握业务处理过程并进行适当的记录，进行流程草图初步绘制。

第二步　根据访谈掌握的情况，详细记录每个步骤业务活动及对应的执行部门、执行岗位。

第三步　指定每个步骤所对应的实施证据。

第四步　将该流程对应的风险标注到每个相关的流程步骤上，如果适用风险无法进行标注，说明流程梳理不完全，应增加相应的流程步骤。

第五步　对存在风险的流程步骤标注控制点。

第六步　在分支流程“流向”一栏中记录流程的前后逻辑关系，如果业务流程复杂，不能清楚反映各流程步骤之间的逻辑关系，可附草图以说明流程步骤的前后关系。

流程梳理是流程描述的一个基本内容也是进行流程描述的前提，流程梳理质量的高低直接影响流程描述的质量，并且对于风险的防范和控制措施的实施具有重要的意义。

4.4.2 业务流程描述

1．业务流程描述的概念及内涵

业务流程描述遵循业务运行实际，结合风险控制要求，描述业务工作步骤，实现业务管理程序化的过程。流程描述的对象是基本业务流程中的末级流程。

它的基本内涵有以下几个方面：

一是流程描述要采取某种特定的方法，如文本法、流程图法。这是业务流程表象化的方式，即把隐含在企业内部的某一互有关联的业务活动以更直观的方式表达出来。

二是流程描述要遵循一定的规范。流程描述不能人为地按照主观意愿来表述，而应该在专家的指导下，在科学地进行业务流程梳理的前提下，突出风险和控制，尽可能使描述出来的流程更加符合业务实际和科学管理的要求。另外由于我们采用了目前比较完善的流程描述系统软件，因此在

描述流程时更应该考虑到系统软件的特殊规定，规范地进行流程描述。

三是流程描述的对象是企事业单位基本业务流程中的末级流程中的业务活动。对于末级流程以上的各级流程无须进行详细描述，一般只是对其进行定义即可。

2．流程描述的原则性要求

（1）整体性要求

① 将本企业作为一个整体对业务流程加以描述。

② 应避免因描述者个人的局限，出现部门间、业务间描述的详略失当。如果在进行流程描述时只片面地关注本部门、本岗位的业务，不能对整个流程有全局的考虑，将使流程描述丧失了整体性，各步骤间丧失了逻辑性和连贯性，并会出现流程的断层、重复或遗漏，造成相关流程之间接口不明，从而影响流程描述整体的质量。

③ 流程图不应只是流程主管部门的职责描述，应全面反映业务活动过程中主管部门、相关部门及所属单位的职责、工作内容和处理业务过程中保存的记录（如文件依据、报告、审批记录、会议纪要等）。绘制跨部门的流程图时，不能只强调主管部门的工作内容，而忽略相关业务部门的参与，应当将业务的不同阶段主管部门及相关部门的工作都全面、准确、完整地反映在流程图中。

（2）完整性要求

① 每个基本业务流程中的末级流程对应一个流程图，不能缺少必要流程。

② 流程图中各种要素要体现完整。下列情况属于要素体现不完整：流程步骤框中无文字；信息系统或软件生成的表单、报告等缺少名称，或不是实际使用中的全称；流程图无流程名称、流程步骤缺岗位名称。

③ 流程图不能缺少必要活动或控制环节，过于简单或内容不全，无法反映业务运行过程。流程图中必须反映每个流程的主要步骤，特别是业务过程中的授权、审核、签字、复核等控制步骤。

④ 各流程步骤都要有对应的实际操作岗位，责任主体须尽可能细化到科室。

⑤ 流程图要做到简洁并通俗易懂，便于读者了解业务、操作，对不易理解或理解易产生歧义的步骤应用注释说明。

⑥ 流程图应该注明必要的表单。流程图中业务操作的文档记录、表单应该表示出来，要能够提供出记录控制活动载体。文件、记录、表单在作为某个流程步骤的重要输入或输出时，必须在该流程步骤进行体现（如×××明细表、×××审批单、交接台账等）。

⑦ 同属一个流程的两个或多个子流程，流程图的结构、流程步骤、内容完全相同、内容完全一致，此情况应考虑归类合并。

⑧ 绘制流程图要注重控制的描述。控制要素要全面，体现谁控制、如何控制、控制的频率、要保存什么控制记录等。

（3）逻辑性要求

① 流程描述逻辑关系要清楚，应避免连线混乱，甚至出现局部死循环现象。

② 流程图所反映业务内容和流程名称应保持一致，不能出现脱节的现象。

（4）一致性要求

① 注意流程内部和流程之间的衔接点。由于流程涉及内容较多，既要注意流程内部的逻辑关系，也要注意流程之间和不同的控制点之间的衔接。接口应在各自的流程中体现，并保持相互一致。

② 流程描述的层次及内容应尽量规范。同一流程图、不同的流程图中，同一文件、部门、岗位的使用必须规范统一，保持高度一致性。

③ 相关流程间的一致性要求。与企业外有业务往来的流程（如采购、销售等）结算付款与财务管理流程中支付结算要衔接一致；统一管理且流程一致的业务活动（如结算、签订合同等）应在一个流程图中集中描述，其他业务流程中相同业务引用此流程；企事业单位内部部门间、与下属单位间的信息传递、上传下达的接口在各自的流程中要体现一致性。

④ 流程之间的引用必须有对应的流程图，可以在流程目录中找到。

（5）关注风险，突出控制，为建立风险控制矩阵做准备的要求

描述流程时，各建设单位应根据本身的具体业务，对业务流程中存在的风险予以关注，特别是对规避这些风险而设置的控制应重点关注，这样便于把握流程步骤的繁简程度。

（6）现状分析与控制改进相结合的要求

如果公司即将实行新的政策，会对业务流程有所改变，那么流程按照实行新政策后的业务流程描述。当实际操作与规章制度相违背时，必须按照制度的要求进行操作并按制度规定描述流程。部门和岗位变化后，需要对相应的流程按调整后的情况进行重新描述。

流程步骤的描述要符合管理现状，是对管理现状的规范性描述，不能脱离现状，不能是理想状态。内部控制建设的最终目标是在对管理现状进行分析的基础上，按照内部控制理论和标准发现存在的问题和不足，提出改进意见，完善内部控制制度，提高管理水平。我们在现阶段业务流程描述时，不仅要分析现状，而且要思考内部控制中存在的问题及如何改进等问题。

3. 流程描述方法分类

流程描述方法主要有两种，即文本法和流程图法。



（1）文本法

文本法采用文字记录的方式（Word 文档），说明一个业务流程从开始到结束的整个过程及相关内容，也叫做流程描述法。

（2）流程图法

流程图是比较流行的方法，主要使用 Microsoft Office 组件 Visio 软件进行流程描述。

下面我们将按照实际操作过程的逻辑顺序介绍业务流程描述的流程图（Visio 图示法）。

4．流程图

流程图是用图形符号和有限的文字叙述来描述步骤性质、流程和关键路径的图表。流程图被用在多个不同领域以记录处理步骤。

（1）流程图的特点

流程图可以使我们更加充分地理解一个流程，从起点到终点（即一项业务的流程），并且使我们更加容易识别控制的薄弱领域及其改进的机会。

流程图也提供了一个全面的系统描述，从而可以被有效地运用在：

① 识别关键的控制。

② 评估系统程序并识别系统中易发生错误的环节。

③ 定义责任范围。

④ 向新员工解释系统及相关控制。

因此在实务中，流程图被广泛使用。

（2）Visio 流程图的构成

① 使用软件。Microsoft Visio。

② 标准流程图模板。模板应用 Visio 中跨职能流程图，如图 4-10 所示。

101 财务报告编制流程	截止时间：2010-2-28	单位：总部
101.01 会计科目维护		最新修改日期：2010-3-15
部门1		
部门2		

图 4-10　Visio 流程图示例

- 表头部分。流程代码及名称，该流程反映的截止时间，所属组织单位，子流程代码及名称，该流程图最新修改时间等。
- 流程图。流程图描述采用横向（纵向一样）垂直方式，自左到右、自上而下表示流程发展的时间或逻辑等顺序。流程图页面设置为横向；纵向以职能带区代表单位或职能部门。单位或职能部门顺序从上到下排序。

（3）图例及说明

如表 4-1 所示。

表 4-1　流程图图例及说明

序　号	图　　例	图例说明
1	负责人员 控制	**负责人员**：填列负责该工作的岗位。**控制**：简要描述人工具体实施的工作步骤，如填写费用报销单
2	负责人员 SAP 控制	**负责人员**：填列负责该工作的岗位。**控制**：简要描述在系统（如 SAP）中完成的业务活动，如系统创建销售订单
3	文档名称	电子文档，内容为其名称

续表

序 号	图 例	图例说明
4		流程目录中已经明确的具体业务流程，此图例表示对其他流程的引用
5	文件、表单的全称	该图例表示纸质文档，包括制度、表单等，内容为文件、表单的全称
6		此图例在存在判断/决策时使用，内容中填列判断的具体事项
7		表示离页索引，内容填列索引的页码编号
8		用来连接两个工作步骤
9		表示在信息系统
10		表示流程开始或结束
11	K	表示业务流程中关键控制点，标识在控制点的右下角，结合编号单位、流程编号、风险序号、控制点序号等进行编号，如K110.01.01……
12	C	表示业务流程中一般控制点，标识在控制点的右下角，结合单位编号、流程编号、风险序号、控制点序号等进行编号，如C110.01.01……
13	K	表示业务流程中IT关键控制点，标识在控制点的右下角，结合单位编号、流程编号、风险序号、控制点序号等进行编号，如K110.01.01……
14	C	表示业务流程中IT一般控制点，标识在控制点的右下角，结合单位编号、流程编号、风险序号、控制点序号等进行编号，如C110.01.01……

（4）范例如图 4-11 所示

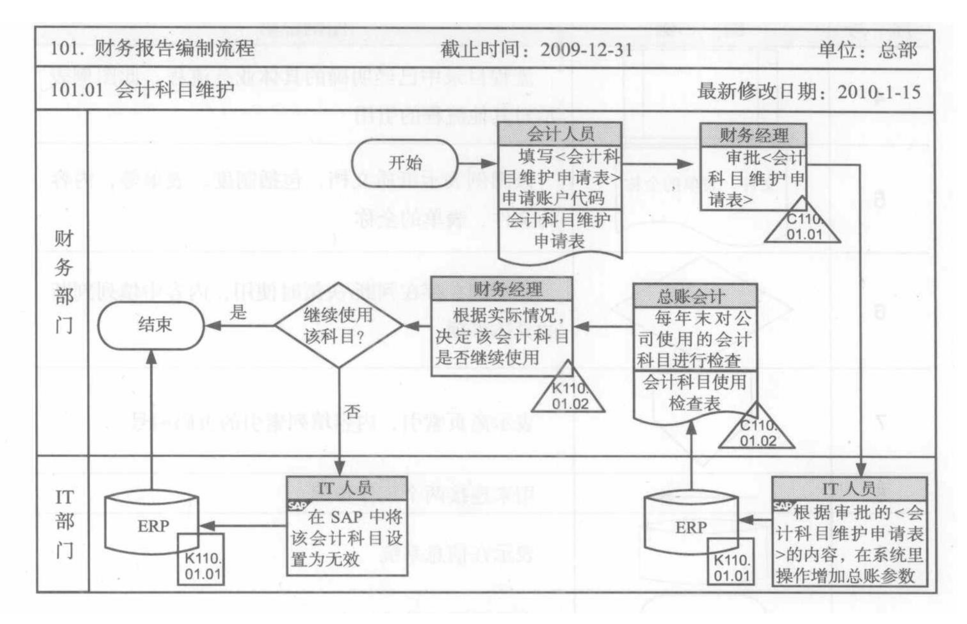


图 4-11　流程图范例

需要注意的是，截止时间表示该流程图反映的是截止到该时间的业务现状。

5．风险控制矩阵的编制

风险控制矩阵（RCM）详细地体现业务流程中存在的风险和控制设计的情况。它是对现有规章制度进行描述和分析的主要载体，也是联结业务流程、风险、现有控制措施、规章制度文件的工具。

（1）风险控制矩阵的作用

通过使用风险控制矩阵，将风险对应到具体的业务流程中，了解在实际工作中如何控制这些风险，并将这个过程文本化。

风险控制矩阵记载并体现了风险控制分析所发现的控制缺陷和不足，是后续进行差异分析、控制完善的重要基础和依据。

风险控制矩阵还是自行测试、外部审计的重要依据。

（2）风险控制矩阵的模板（如表 4-2 所示）

表 4-2　风险控制矩阵模板

<table>
<tr><th colspan="18">风险控制矩阵（RCM）</th></tr>
<tr><td colspan="8">流程编码及名称：
截止时间：
编制部门：</td><td colspan="10">子流程编码及名称：
版本：
编制人：</td></tr>
<tr><th rowspan="2">控制点编号</th><th rowspan="2">控制目标描述</th><th colspan="4">风险类别</th><th rowspan="2">风险描述</th><th rowspan="2">关键控制编号</th><th rowspan="2">现有控制措施</th><th rowspan="2">控制方法（自动/人工）</th><th rowspan="2">控制类型（预防性/发现性）</th><th colspan="2">应用系统控制</th><th rowspan="2">控制频率（随时/日/周/月度/季度/年度）</th><th rowspan="2">控制实施证据</th><th rowspan="2">控制文件名称</th><th colspan="2">适用单位</th></tr>
<tr><th>战略风险</th><th>经营风险</th><th>报告风险</th><th>合规（法律）风险</th><th>所属应用系统/模块</th><th>相关控制措施</th><th>总部</th><th>下属公司</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

（3）风险控制矩阵编制说明

依据流程描述、控制活动涉及的规章制度及风险数据库进行风险控制矩阵的编制。

风险控制矩阵选用 Excel 文档形式进行描述，文档的名称为《风险控制矩阵（RCM）》，用以确认、记录存在风险的流程步骤的现有控制措施及相关要素的文档。

1）表头说明

表头中，均为必填内容，如实填写即可。其中，“最后更新时间”指修

改该风险控制矩阵的最新时间，“版本”主要是根据内容的更新进行版本控制。

2）表体部分

① 控制点编号。与相关流程图上的控制点编号一致。控制编号以小数点为界，分成三部分：第一部分为流程编号；第二部分为风险序号；第三部分为风险控制类型和控制点编号。例如，C108.01.01，其中 C 表示控制点，Control，1 代表单位编号；08 代表流程编号；01 代表该流程的风险序号，01 代表该风险点的手工控制序号。所有的控制点均应进行编号；控制点编号必须和流程图中的编号对应。

② 控制目标具体描述。说明该项控制要达到的目标。根据所选的控制目标的类型，具体描述针对风险的控制目标。

③ 风险类别。根据《内控规范》的要求，结合公司目标，将风险分为战略、经营、报告和合规（法律）风险四类。根据风险描述，结合对应的目标，确定风险类别。

④ 风险描述。与目标对应，与目标描述内容相反，参考风险数据库的内容，对风险的内容进行详细描述，根据本单位的实际情况进行风险识别和描述。若对风险数据库进行调整，特别是增加的风险，该风险描述要明确具体地描述影响目标实现的因素。

⑤ 关键控制编号。以小数点为界，分成三部分：第一部分为流程编号；第二部分为风险序号；第三部分为关键控制点编号。例如，K108.01.01，其中 K 表示关键控制，Key Control，1 代表单位编号；08 代表流程编号；01 代表该流程的风险序号，01 代表关键控制点序号。

⑥ 现有控制措施。详细描述实际采用的控制措施，需满足五要素，即“谁（Who）”、“为了达到什么目标（Why）”、“在什么时间（When）”、“在

什么地方（Where）”“做了什么事（What）”。

⑦ 控制类型。控制活动可以是预防性的或发现性的。

预防性控制是防止问题发生的机制；在风险发生之前，为避免风险采取的措施。例如，制定政策、准备备查清单、合同在执行前需要审批等为预防性控制。

发现性控制是为发现问题而设立的控制机制；事后做的、为及时发现问题而采取的措施是发现性控制。例如，核对财务系统和资产系统的余额是否一致，审核记账凭证是否准确，编制银行存款余额调节表等。

⑧ 控制方法。控制活动可以是人工的，也可以是自动的。

人工控制如人工核对，授权签字，信用状况核查和信用限额批准等。

自动的控制如操作系统登录和权限控制；超出信用额度，系统自动限制发出货物及开出发票；自动校验等。

⑨ 应用系统控制，是嵌入在业务流程控制中的。“所属应用系统/模块”指承载该应用系统控制的 IT 系统或者某个比较大的系统中的某个模块，如 SAP 中的 FI（财务）模块。“相关控制措施”详细描述这个应用系统控制，要注明控制方式，如数据类型校验、重复输入校验、批总量控制、序列校验、系统匹配、逐一检测、编辑校对、预定的数据列表、授权检查、有效性检查等技术控制。具体内容将在“4.5IT 应用控制”中介绍。

⑩ 控制频率。说明该控制多久、什么时候控制一次，分为随时/日/周/月度/季度/年度。

⑪ 控制实施证据。指在实施现有控制时所使用的报告、表单、签字等，最能说明或证明执行过某项控制的书面证据。这里的证据范围较广，可以是统一实施证据，也可以是会议记录或电话记录等。如果在实施现有控制时没有使用相应的报告、表单、签字等，则应填“无”。

⑫ 控制文件名称。指该项控制的管理制度文件的名称。若没有控制文件，则应填“无”。

⑬ 适用单位。指该项控制适用的组织单位。适用于总部，或者适用于下属某些公司，或者全部适用。

风险控制矩阵编制时所涉及的支持控制的制度文件，包括公司及其下属公司下发的各项规定、要求、管理办法、实施指南、意见、通知等各个类型的制度文件，以及国家相关法律法规和政府管理部门下发的制度文件。

6. 穿行测试

穿行测试是了解业务现状和内部控制设计的有效途径。实践中，穿行测试（Walkthrough）也是更新与完善流程图和风险控制矩阵（RCM）的有效方法。

（1）穿行测试的定义

对每类重大交易中选择一笔交易，从其起始进行追溯，通过公司的业务流程与IT系统，一直到其结束。需要注意的是，我们选择一个样本，应从头至尾穿行，也就是要保证在流程各个环节获取的文档要能钩稽起来。

（2）穿行测试的目的

① 熟悉和理解业务流程。

② 验证公司确认的关键风险和关键控制的完整性和合理性。

③ 验证关键控制设计的有效性，即公司确定的关键风险和关键控制在被测试单位是否被采用，如果没有被采用，分析其合理性；被测试单位业务流程中存在的特殊重要风险是否被识别，相应的关键控制是否被确认并准确记录。

④ 检查被测试单位是否制定了与控制实施相关的制度。

⑤ 确认控制（一般控制和关键控制）是否被有效执行，该控制执行后能否防范风险。

⑥ 找出流程描述和风险控制矩阵的内容与实际执行情况的差异，分析差异产生的原因，并提出整改完善建议，使内部控制文档和实际情况保持一致。

（3）穿行测试的步骤

1）访谈

访谈原则上要求就实施控制的每个岗位进行访谈，以确保获取最直接的信息。但如果测试人员能够肯定判断从一个或几个岗位上访谈所获取的信息已经足够支持测试所需了解的内容和信息，那么根据被测试单位的实际情况，可以不用访谈每个岗位。

访谈时重点关注：

- 公司确定的关键风险和关键控制在被测试单位是否被采用，并在哪些岗位实施。
- 被测试单位业务流程中存在的特殊重要风险是否被识别，相应的关键控制是否被确认并准确记录。
- 了解以前年度存在的问题的整改情况，并在设计层面初步分析整改后是否达到了控制目标，分析其合理性。

2）选择测试样本

① 样本选取的方法。审阅流程图和风险控制矩阵描述的相关文档记录是否存在，如果存在，样本一般按流程描述的先后顺序抽取一笔业务从流程开始追踪至流程结束。为提高测试效率，也可以采取业务发生的逆顺序的方式进行样本的选取。不管采取哪种方式，都应保证所选取的样本能够贯穿业务流程全过程，同时注意应在不同业务部门取得与样本相关的证据

资料。

如果流程中有因审批权限、业务性质等不同产生的流程分支，由于前段流程相同，所以选取不同的分支样本，只需测试在分支阶段不同的控制，而不需要再依据不同分支取得的样本从头测试一遍。

针对不同业务流程中的引用流程（如合同签订、会计核算、资金支付等引用流程），测试人员不需要进行重复的穿行测试。但是测试人员应该相互之间进行充分的沟通，做到对重要流程步骤的不遗漏，以确保测试范围的完整性。

② 选择样本需考虑的因素：

- 能够代表重要业务流程中的主要业务类型，具有一定的普遍性。
- 同一业务流程中，IT 应用控制选取的样本与手工控制选取的样本必须对应相同的业务事项。

3）检查控制是否存在并执行

对选定的样本进行检查，重点关注以下方面：

① 被测试单位设计的控制是否被有效执行，该控制执行后能否防范相关的关键风险；进而验证访谈结果是否准确，即公司确定的关键风险和关键控制在被测试单位是否被采用，并在哪些岗位实施；被测试单位业务流程中存在的特殊重要风险是否被识别，相应的关键控制是否被确认并准确记录。

② 检查相关文档记录是否按要求填写和传递。根据文档填制情况，分析描述的控制在实际工作中是否得到执行，实际执行中的控制在风险控制文档中是否进行了相关的描述，实际执行的控制是否留下实施证据。

③ 在检查样本时，应结合公司设计有效性测试及被测试单位设计有效性测试发现的问题，通过检查样本进一步验证设计方面发现的问题。对执

行层面发生的缺陷应分析其产生的原因，是否是因为设计方面存在问题而产生缺陷。

4）观察

对正在发生的特定控制进行观察，进而获取控制证据。例如，在票据管理流程中，一般都存在《票据与银行印鉴分开保管》的控制，针对该控制可以执行的测试步骤是：观察银行预留印鉴是否由出纳岗之外的其他人员分开保管。

5）记录测试情况

测试完毕后，根据测试结果记录测试过程，包括访谈的岗位，观察的事项、时间、结论，检查的相关样本，记录发现的问题，并复制缺陷涉及的相关证据。

6）完善文档与整改建议

经过穿行测试，找出流程图和风险控制矩阵的内容与实际执行情况的差异，分析差异产生的原因，并提出整改完善建议，更新完善流程图和风险控制矩阵等内容，确保与实际情况保持一致。

7. 差异分析与完善

（1）补充识别评估风险

在完成流程图和风险控制矩阵编制工作后，在穿行测试过程中，按照公司制定的风险评估方法和标准及风险数据库，结合实际业务，对主要业务流程开展风险评估的补充识别、评估工作。从风险入手，考虑影响目标的具体问题，讨论存在的风险。对于新识别的风险及控制，参照有关定义，或者参考风险数据库对其做出界定，将新识别的风险和需要对风险数据库调整的具体内容，经审批后补充完善到风险数据库中。

（2）识别、确定与风险相应的有效控制

针对风险数据库中的风险，对现有文件、制度规定及实际业务执行中的相应控制措施进行分析，分别找出风险对应的控制。

1）控制与一般业务活动的区别

控制是为防范和规避风险，保证管理层的指令、政策得以执行的必要措施或程序，按作用分为预防性和发现性控制。

控制与一般业务活动过程的区别就在于：控制具有预防性或者发现性；同时每项控制的设计、实施总是针对特定的某个或某几个风险而为，因而还具有针对性。表 4-3 是两者区别的一些实例。

表 4-3　控制与一般业务活动的区别

序　号	业务程序	控制/活动
1	从 EPP 系统中，打印所有付款金额、付款人相同的支票的报告，即疑似重复付款报告	活动
2	将付款期为一年以上的账款单独分类	活动
3	审核系统安全设置，确保录入订单的权限被严格控制	控制
4	审核所有超过五千元的发票，确保得到部门经理的适当批准	控制
5	核对收到货物的收货数据与采购订单数据	控制
6	确定采购折扣	活动

业务 1、2、6 没有任何跟进措施（如审核等）的活动，没有实现预防或者发现的作用，不属于控制。

2）内部控制设计有效性评价

针对风险设计的控制是否有效，可以从以下几个方面判断：

- 控制是否与企业的业务流程及相关风险相匹配。
- 控制是否接触满足完整性、准确性、有效性和性的要求。
- 控制是否能够及时发现和预防风险（控制实施的频率）。

- 控制实施人员是否有足够的知识和经验。
- 是否实施职责分离。
- 控制中发现的问题是否能够及时得到处理。
- 在实施控制中所使用的信息是否可靠。
- 控制是否适应环境的变化。

参考表4-4来判断控制的效果，这里指的效果只是相对而言。

表4-4　控制效果分析

控制效果	
强	弱
IT控制	人工控制
简单控制	复杂控制
有经验的人员	缺乏经验的人员
预防性控制	发现性控制
多层次控制	单一层次控制
业务层面的控制	公司层面的控制
事前/事中控制	事后控制

3）识别内部控制设计缺陷

控制活动在设计上，不能有效地防范或减少控制点风险，表示是内部控制弱点。一般有下面两种情况。

① 有风险，无控制。例如，我们都知道报销费用的时候，要找领导签批，领导审核、签字的这个过程就是对费用的一个控制。如果我们在设计内部控制的时候没有设计这个程序，没有要求费用需要相应的领导签批才能报销，随便一个人都可以到财务那里报销，随便报。很快公司的资金就会被报销完了，公司运转不下去，要倒闭了。这就是有风险，无控制。

② 有风险，控制不足够。如果我们内部控制设计的时候，设计了费用报销的审核、签字，但是只是要求自己审核一下，签个字就行了，那么这个控制没有意义。执行完这个控制后，公司倒闭的风险一点也不会减少。这是有风险，控制不足够。

4）完善内部控制设计

针对发现的内部控制设计缺陷，提出整改建议，完善公司内部控制设计。

① 有风险无控制的，寻找替代控制，或者建立控制，然后在流程图和风险控制矩阵中添加相应的控制。

② 有风险，控制不足够的，寻找补充控制，或者完善该控制，然后在流程图和风险控制矩阵中添加相应的控制。

例如，合同签订流程中，由于对合同专用章被盗用的风险没有控制，应增加相应控制措施，并在流程图中增加此控制，即为“加盖合同专用章时应登记合同专用章台账”。

5）完善文档

经过文档编制、穿行测试、差异分析、内部控制设计完善后，需要对相关的文档进行完善。

① 流程图是业务流程的直观、概括的体现。通过图中的风险点和控制点与风险控制文档相链接。

② 风险控制矩阵详细的体现业务流程中的风险和控制设计的情况。它是内部控制描述的主要载体，亦是联结风险、控制、制度文件、差异分析结果的工具；是后续进行控制完善、差异分析及控制测试的重要基础和依据。

4.4.3 确认关键控制

1．确认关键控制的目的

关键控制是公司在经营管理中，为了防范重要风险而制定的重要的、最有影响力的一项或多项控制。如果缺少这些控制，将会在很大程度上产生财务报表错报、资产安全受到威胁、舞弊和较大经济损失的风险。

关键控制确认是在前期全面进行风险评估、控制分析的基础上，为了强化控制活动，突出控制重点，简化评估测试而开展的一项重要工作。关键控制是内部控制体系框架的重要内容，是实现控制目标的最重要的控制措施，也是外部审计师关注的重点审计内容。

通过关键控制确认，一是突出控制重点；二是可以为管理层测试内部控制体系的完整性和有效性提供统一的范围和标准；三是可以为外部审计师评估、测试公司内部控制体系完整性和有效性提供基础性资料。

2．确认关键控制的基本标准

① 确认的关键控制，是在相关流程中影响力和控制力相对较强的一项或多项控制，其控制作用是必不可少和不可替代的。如果缺少该项控制，将在很大程度上直接（而不是间接）导致风险的产生。

② 确认的关键控制，对应风险是根据风险评估的结果确定关键风险。

③ 确认的关键控制，必能实现一项或多项控制目标，而且同时满足多项控制目标的控制更关键。

④ 确认的关键控制，必须存在控制证据并能够对控制过程进行验证和测试。

3．确认关键控制的程序

① 内部控制项目组提出相关业务流程的“关键控制点和控制要点”，

形成“关键控制管理文件”。

② 将关键控制管理文件发给公司相关部门、下属公司全面征求意见，项目组根据反馈的意见，按照关键控制确认标准，修订完善。

③ 如有必要，可聘请外部的专业咨询机构支持。

④ 项目组将修改后的关键控制管理文件提交公司相关部门、下属公司进行确认。

⑤ 将关键控制管理文件提交公司领导审批，成为公司制度文件。

4.5 IT应用控制建设

4.5.1 应用系统的划分

如果公司使用的应用系统很多，需要按对公司业务流程的影响程度对信息应用系统进行划分。实际操作中，主要是根据应用系统跟财务报告的关系来划分，在第2章中曾有介绍。

1. 应用系统划分标准

在对应用系统进行等级划分时，考虑以下因素：

① 是否在公司范围内普遍使用。

② 是否存在对财务报告产生重大影响的会计科目。

③ 是否存在对财务报告产生重大影响的功能（重大影响的功能是指直接或间接对财务报告与披露数据产生重大影响的应用系统功能模块）。

④ 与财务系统的数据交换方式（手工或自动、数据范围）。

⑤ 是否可在所有重大方面依赖手工控制。

2. 应用系统划分

（1）重要应用系统

将满足以下条件的应用系统，划分为重要应用系统：

① 在公司范围内（包括下属公司）普遍使用。

② 存在对财务报告产生重大影响的会计科目，或存在对财务报告产生重大影响的功能，或与财务系统的数据存在接口（手工或自动）。

③ 在重大方面无法依赖手工控制。

（2）普通应用系统

将同时满足以下四个标准的系统，确定为普通应用系统：

① 存在对财务报告产生重大影响的功能。

② 存在对财务报告产生重大影响的会计科目。

③ 在公司范围内较普遍使用。

④ 所有重大方面可以依赖手工控制。

（3）其他应用系统

重要应用系统与普通应用系统以外的应用系统划分为其他应用系统。

3. 应用系统控制内容

（1）重要应用系统

识别应用系统控制并对关键应用系统控制进行测试。

（2）普通应用系统

识别与普通应用系统相关的手工控制，并判断相关手工控制措施是否可保证财务数据的真实、准确与完整。若无法满足，则

① 增加或改善的手工控制。

② 在无法增加或改善手工控制的前提下，识别普通应用系统控制。

③ 其他应用系统。

（3）不进行应用系统控制识别与测试

4.5.2 应用系统用户权限管理

1. 应用系统用户权限管理的基本原则

用户权限管理应同时满足以下基本原则：

① 需求导向及最小授权原则。对于用户的权限，应当以其实际工作需要为依据，且仅应当授予能够完成其工作任务的最小权限。

② 未明确允许即禁止。除非用户对权限的需求得到了相关领导的明确批准，否则不应当授予用户任何权限。

③ 职责分离原则。任何一个用户不能同时具有两种（或两种以上）的不相容权限。

2. 应用系统用户权限管理的组成

① 访问控制。是指用户能够访问哪些应用系统内的资源或执行哪些任务（或功能）的范围，从控制的角度考虑在系统中所拥有的功能权限和数据权限是否超出了其工作需要。

② 职责分离。职责分离是把一个业务（子）流程的工作内容分为几个职责不相容的部分并由不同的人来完成，避免因同一个人能够操作不相容职责而产生的错弊风险。

3. 应用系统用户权限管理

（1）将职责分离融入应用系统用户权限中

依据不相容职责分工的原则，从业务流程和组织结构层次两个维度进

行分析，可以定义出系统中的冲突权限。

① 从业务流程的维度（横向）出发，需要职责分离：

- 交易的发起，如凭证录入。
- 交易的复核（或授权），如凭证复核。
- 交易的记录，如凭证记账。
- 实物保管，如出纳。
- 稽核检查，如内部审计。
- 主文件维护，如数据中心的核算对象维护。
- 系统管理，如系统运行参数维护。

② 对于规模大企业，需要考虑由企业组织结构中不同层面的人完成的职责，也应当视为必须分离的职责。

例如，通过系统审批合同，根据公司权限，大于1亿元人民币的合同，系统内容的录入、下属公司审核、总部审核、总部合同管理部门领导审批、总部主管副总裁审批五种权限之间属于不相容权限。

（2）形成应用系统用户权限体系

结合公司实际业务流程需要，根据应用系统用户权限管理的基本原则，按照应用系统权限实现方法，在应用系统内形成完整恰当的应用系统用户权限体系。

（3）应用系统用户权限测试

在建立完成应用系统用户权限体系后，需要对权限在测试环境（Testing）中进行测试，发现问题及时调整。

（4）应用系统用户权限确认与运行

经过测试环境测试无误后，将权限清单交由用户签字确认后，领导审批后生效。将测试环境（Testing）转入生产环境（Production），权限体系

正式运行。

4．权限日常管理

权限日常管理是依据应用系统用户权限，对用户权限的申请、审批、变更、删除进行管理。

（1）应用系统用户增加

在系统新增用户时，根据以下步骤设置用户的权限：

① 根据企业的组织结构、岗位设置等，明确用户的岗位职责。

② 依据功能权限和数据权限的标准，从负责授权的业务部门主管（或信息部门主管）取得正式批准。

③ 在系统中为用户设置相应的功能权限和数据权限。

④ 在与系统相对应的“通用角色与系统终端用户对照表”中增加该用户的信息。

（2）应用系统用户变更

在用户的工作内容发生变动情况时（不包括离职），根据以下步骤调整用户的权限：

① 根据企业的组织结构、岗位设置等，结合调整的内容，明确用户新的岗位职责。

② 依据功能权限和数据权限的标准，确定授权的调整范围，从负责授权的业务部门主管取得变更的正式批准，并以书面形式记录变更和审批过程。

③ 在系统进行相应权限的授权。

（3）应用系统用户离岗/离职

在用户离岗（离职）时，根据以下步骤调整用户的权限：

① 用户办理离岗（离职）手续必须有应用系统管理部门签字确认。

② 签字确认前，系统管理员查看该用户在系统中的权限并及时禁用（或删除）用户 ID。

5. 特殊权限的管理

（1）特殊授权类管理权限

在应用系统中，有些必须的、不经常使用、对系统至关重要的功能，通过这些功能的设置，可对系统的运行产生重要的影响。这些需要特殊授权的权限（如 SAP 中的“折旧参数维护”等）和岗位在日常不应当授予任何人员，而是在具体工作需要时，必须在履行严格的申请、审批和授权流程后，并由系统的管理员临时授权，使用完毕后，应马上收回授权。

（2）禁用的权限

在有些系统中设有“凭证删除”的权限，即拥有此权限可以删除已经生成的会计凭证。由于凭证删除不符合有关会计核算的规定，因此应当禁用此功能，不允许授予任何人。

6. 权限定期审阅

在日常的管理工作中，应当定期对用户在系统中的访问权限进行检查，主要有：

① 定期（如 6 个月）或在发生变动后，检查所有用户权限的设置情况。

② 对于拥有关键权限的所有用户，应当以更短的周期（如 3 个月）定期进行检查。

7. 权限变更流程

在应用系统的用户权限发生变动时，应当按照 IT 一般控制中相关的流

程进行变更处理。特别需要注意的是：对于特殊授权类权限，需要在使用完毕后及时收回。对于临时权限申请期限，由于各类业务性质的不同，无法明确一个固定的期间，需要申请和审批人根据具体的操作业务种类和性质确定申请期限（对于临时授权期限要根据实际业务内容和工作量进行衡量判断），管理员按照该期间及时收回权限。

4.5.3 应用系统自动控制

1．应用系统自动控制方式

信息系统可利用数据类型校验、重复输入校验、批总量控制、序列校验、系统匹配、逐一检测、编辑校对、预定的数据列表、授权检查、有效性检查等技术控制，对应用系统的输入、处理和输出进行有效控制。

（1）对输入数据的确认

应用系统如果受到故意或意外无效数据的攻击，会导致系统故障、数据滥用或通过系统本身安全漏洞进行欺诈犯罪等事件的发生。因此应用系统采用数据确认控制将数据的输入范围控制在一个合理的范围内，即限制在系统有效处理能力之内。

① 定期评审关键的数据文件的内容，确保其有效性和完整性。

② 检查硬拷贝的输入文件，确保输入数据没有经过任何未经授权的更改。

③ 建立错误数据的相应程序。

④ 建立程序对于可怀疑的数据进行进一步检查。

⑤ 规定数据输入过程中所涉及的所有人员的职责。

（2）对数据内部处理的控制

已经正确输入的数据也可能因为处理的错误或人为的改动而被破坏，

因此为了保证数据在处理过程中的安全性，应对数据处理进行以下控制：

① 批处理控制，确保事务更新后保持数据文件的平衡一致。

② 确认系统产生数据的正确性。

③ 确认数据传输过程中的完整性。

④ 检查确保应用系统运行的时间正常。

⑤ 检查确保应用系统运行的顺序正常。

（3）对输出的数据进行确认

尽管系统的输入是正确的，但输出仍然可能是错误的或是经过非法修改的。为确保输出信息的正确性，要对输出的数据进行确认，主要包括：

① 可信性检查，确认输出的数据是否合理。

② 数据一致性检查。

③ 相应输出确认测试的程序。

④ 数据输出过程中相关人员的责任。

（4）例外处理

相关岗位的操作人员对操作过程中出现的例外活动，根据情况将例外事件情况及时汇报给主管领导进行处理。

2．应用系统控制识别

（1）应用系统控制的概念

在系统控制中将 IT 与内部控制相结合，主要涉及系统安全和系统运行两方面内容。系统安全主要包括：网络安全、应用系统安全、数据安全等。系统运行主要包括：程序设计、运行维护、用户访问、审核验证、身份确认、系统应变控制与设置、不相容职务的设置与验证及信息系统基础环境的设置和验证等。

应用系统控制是内部控制体系建设的重要组成部分，也是内部控制体系检查的重要工作内容之一。

（2）应用系统控制的形成

在日常流程管理中，建立了内部控制，有很多的审批手续、监控手续，建立了很多的一些管理的措施，这些措施，除了我们的手工流程以外，跟系统非常相关。各应用系统的审批、授权，这些都是内嵌的业务流程，这些控制是属于应用系统相关的一些控制措施。部分由手工控制的风险点由于在手工流程中引入信息系统管理后，将原手工控制升级为应用系统进行自动控制。

例如，会计业务处理对记账凭证的编制和录入不完整、不准确的应用系统控制为：只有借贷方金额相等的凭证才能被系统生成并保存。

3. 应用系统控制文档

参考“4.4 业务层面内部控制建设”的内容。实务中，业务流程的手工控制与应用系统控制融合在一起。

4. ERP 应用系统控制

（1）ERP 简介

企业资源规划系统（ERP）是一个集成系统，它整合了企业财务、销售、采购、人力资源管理等多方面的资源。以广泛使用的 SAP R/3 为例，系统模块（含 BASIS）包括财务（FI）、成本管理（CO）、生产计划（PP）、存货和采购（MM）、销售（SD）、人力资源（HR）等模块。

各模块功能如下。

FI 财务会计模块　集中公司有关会计的所有资料，提供完整的文献和

全面的资讯，同时作为企业实行控制和规划的最新基础。

CO 管理会计模块 是公司管理系统中规划与控制工具的完整体系，具有统一的报表系统，协调公司内部处理业务的内容和过程。

PP 生产计划 提供各种制造类型的全面处理：从重复性生产、订制生产、订装生产，加工制造、批量及订存生产直至过程生产，具有扩展 MPR Ⅱ的功能。另外还可以选择连接 PDC，制程控制系统，CAD 和 PDM。

MM 物料管理模块 以工作流程为导向的处理功能对所有采购处理最佳化，可自动评估供应商，透过精确的库存和仓储管理降低采购和仓储成本，并与发票核查相整合。

SD 销售与分销模块 支持销售和分销活动，具有出色的定价、订单快速处理、按时交货、交互式多层次可变配置功能，并直接与赢利分析和生产计划模组连接。

HR 人力资源管理模块 采用涵盖所有人员管理任务和帮助简化与加速处理的整合式应用程式，为公司提供人力资源规划和管理解决方案。

（2）ERP 控制类型和控制点

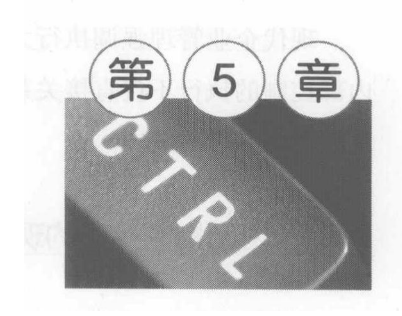
ERP 系统控制，一般可以分为以下类型。

- 配置性控制 需要根据每个企业的实际业务情况和管理要求进行相应的客户化配置，才能达到企业的业务和管理需要，这些控制配制后可以自动实现，如必须关联采购订单才能进行收货操作。
- 流程性控制 虽然 ERP 提供了相当数量的自动控制，但是部分 ERP 自动控制仍然要结合业务流程中的控制才能进行完整的业务操作，如月末结账流程。
- 权限类控制 ERP 为集成系统，所有公司的用户权限在同一套应用系统中进行管理。用户根据拥有的 ERP 适当权限才能进行相应的业

务操作，如A公司的用户不应有B公司的业务操作权限；B公司销售部门的用户不应有财务过账的权限。

- ERP固有控制　ERP提供的标准功能，如采购订单的金额根据采购订单数量和价格自动计算得出。

ERP有助于自动控制取代部分手工控制。例如，信用控制，系统设置好后，超过信用额度的订单就会被系统自动冻结。



内部控制执行与维护

5.1 内部控制执行

现代企业管理强调执行力，执行力就是竞争力，内部控制更是如此。内部控制的执行不仅直接关系控制活动的效果，更影响着企业在复杂竞争环境中的生存与发展。

5.1.1 内部控制执行的现状

1．内部控制执行的重要性

内部控制执行，对发挥内部控制体系的作用、为企业实现目标提供合理保证至关重要。

① 从内部控制本身的定义来看。内部控制本身就包括内部控制设计与内部控制执行两个方面。根据《内控规范》，内部控制是“由企业董事会、监事会、经理层和全体员工实施的、旨在实现控制目标的过程”。它强调的是控制过程的实施和内部控制制度的落地。因此，执行是内部控制的重要内涵和根本要求，绝不能将内部控制看成一堆制度。

② 从内部控制执行本身来看。内部控制体系建设目标是生产优质的产品的话，那么内部控制执行就是管理层和员工按照规程（内部控制设计）开动设备、运转流水线、控制质量、生产产品的过程。由此可见，规程设计得再完善，如果没有严格按照规程操作，要么生产不出产品，要么生产的产品不符合质量要求。换而言之，一套“看上去很美”的内部控制体系如果得不到执行或执行不到位，就会成为一纸空文，也就不可能对企业防范风险和实现经营目标发挥保证作用，也就失去了存在的价值，无端增加

企业成本。

③ 从企业所处的环境来看。随着经济全球化，企业内外部环境变化莫测，企业竞争空前激烈。公司面临着内外部影响目标实现的诸多不确定性和风险。面对这些可能的风险，包括在内部控制执行过程中遇到新问题和新情况，只有未雨绸缪，建立并切实有效地执行内部控制体系，才有可能最大限度地化解风险或减少风险造成的损失，确保公司目标的实现。

2. 内部控制执行存在的主要问题

虽然大家都认为内部控制在提升管理水平和防范经营风险方面的作用毋庸置疑，但是在内部控制执行方面还是存在不少问题。“走形式”几乎成为我国企业内部控制体系建设和实施过程中的一个通病。不少公司看似对内部控制很重视，甚至花钱请咨询公司，制定了一大堆的内部控制制度，以为这样内部控制就很好了，其实那只是一个制度合集罢了，与真正的内部控制相差甚远。

① 内部控制流于形式。有的企业虽然建立了内部控制制度，但只是将制度“写在纸上、贴在墙上、挂在嘴上、没有具体落实在行动上”，形成了说和做“两张皮”。

② 内部控制的刚性不足。一些企业在处理业务时不完全按规定的内部控制程序和标准执行，总是强调灵活性和具体情况具体办理，动不动就是“内部控制制度不符合实际情况，按照内部控制制度做，没法做生意”。特别是，很多企业领导不管在接受外界媒体采访，还是公司内部会议上，都再三强调非常重视内部控制，但实际上，他们往往逾越内部控制，导致上行下效，内部控制随意遭到践踏。

③ 缺乏内部控制执行的激励约束机制。在内部控制实施过程中，相当

一部分企业没有将内部控制的执行情况纳入业绩考核评价和奖惩制度体系中，在很大程度上降低了内部控制的效能。

要想解决上述问题，内部控制体系有效运行、有力执行是关键。

5.1.2 内部控制执行的内容

按照控制活动的要求，从系统控制出发，内部控制执行主要包括以下工作内容。

1. 健全内部控制组织机构，明确职责权限

《内控规范》第十二条规定："企业应当成立专门机构或者指定适当的机构具体负责组织协调内部控制的建立实施及日常工作。"《内控规范》第十四条规定："企业应当结合业务特点和内部控制要求设置内部机构，明确权责权限，将权利与责任落实到各责任单位。"

实施内控规范不是一次性实现的目标，内部控制体系建设是一个长期持续不断完善的过程，它必须能有机地融入一个公司的组织框架体系。由管理层关键成员（通常是首席执行官、首席财务官）领衔内部控制组织体系，并得到审计委员会大力协助，确保管理层的决心与投入是持续不断的，这对于建立有效的内部控制体系至关重要。

在第 4 章我们介绍了内部控制组织体系，根据《内控规范》要求，内部控制组织体系及职责权限如图 5-1 所示。

为了不断适应内外部发展变化，公司内部控制的组织体系需要不断健全和完善，为内部控制有效运行提供保证，完善公司管理，为实现公司目标保驾护航。

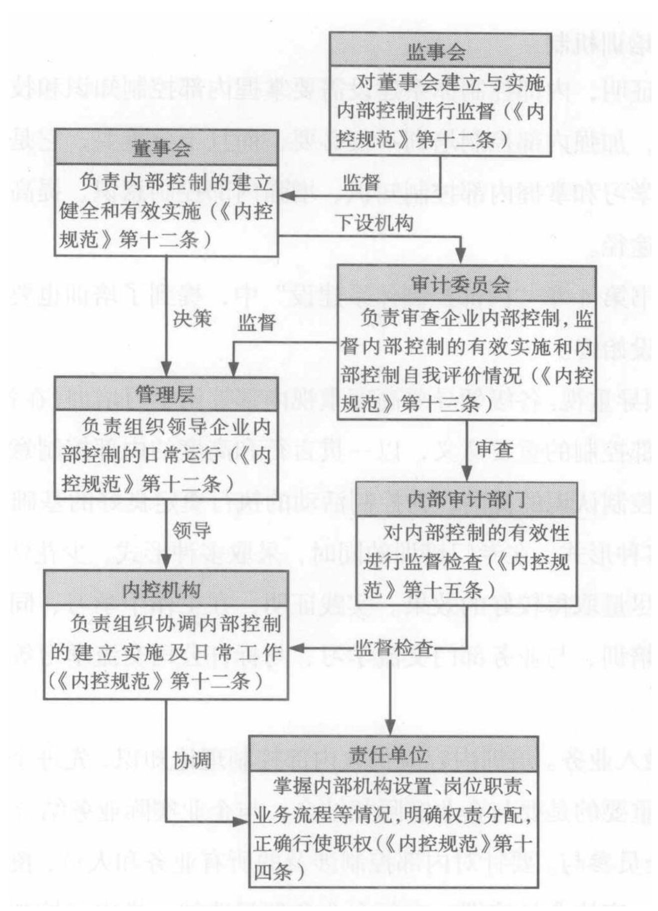


图 5-1　内部控制组织体系及职责权限

2．完善内部控制执行机制

完善内部控制执行机制主要是围绕保障控制活动的实施，建立并运行一整套立足激励与约束、目标明确、逻辑关系清晰的工作制度、程序、办法和措施。根据控制活动的需要，内部控制执行机制包括培训机制和监督检查机制，两者相辅相成，共同构成内部控制执行的执行机制。

（1）培训机制

实践证明，内部控制体系建设需要掌握内部控制知识和技能的员工队伍。因此，加强内部控制培训不仅必要，而且十分重要，它是营造内部控制氛围、学习和掌握内部控制知识、增强内部控制意识、提高内部控制能力的有效途径。

在本书第 4 章“内部控制体系建设”中，提到了培训也要贯穿内部控制体系建设始终。

① 领导重视。各级领导要高度重视内部控制学习培训，在各种会议上，要强调内部控制的重要意义，以一贯言行和高度的内部控制意识，带动员工对内部控制认识的提高，为控制活动的执行奠定良好的基础。

② 多种形式。在专门培训的同时，采取多种形式，少花钱，少占用工作时间，尽量取得较好的效果。实践证明，在工作中学习、同事间相互交流、交叉培训、与业务部门交流学习、与标杆公司交流学习等，都是很好的形式。

③ 融入业务。培训内容应包含内部控制理论知识、先进企业的经验分享等，更重要的是要与企业实际相结合，与企业实际业务结合起来。

④ 全员参与。要针对内部控制涉及的所有业务和人员，覆盖全员和经营全过程，实施全员培训，在每个业务部门造就一批内部控制专家，更好地将内部控制与业务融合起来。

（2）监督检查机制

内部控制监督检查是内部控制的有机组成部分，是促进内部控制有力执行的重要手段。无论美国的《萨班斯法案》还是我国的《内控规范》，都对实施内部控制监督检查做出了明确规定。COSO 于 2009 年 2 月 4 日发布了《内部控制系统监控指南》（*Guidance on Monitoring Internal Control*

Systems），帮助企业有效地执行内部控制监督。

1）监督检查内容

公司内部控制监督检查机制，核心内容为持续监督、独立评估、缺陷报告和整改。

持续监督是在日常经营过程中进行的，包括日常的管理和监督活动，以及员工在履行职责时所采取的检查内部控制执行质量的行为。持续监督分为日常监督和专项监督。日常监督是指企业对建立与实施内部控制的情况进行常规、持续的监督检查，如财务部门对费用的审核、领导的审批等，内部控制机构日常监督和综合考核等；专项监督是指在企业发展战略、组织结构、业务流程、关键岗位员工等发生较大调整或变化的情况下，对内部控制的某一或者某些方面进行有针对性的监督检查。持续监督体现了经常性和持续作用，是内部控制监督检查的重要基础。

独立评估是独立于控制活动之外而采取的定期评估行为。它是基于持续监督，由内、外部审计机构针对内部控制体系运行是否有效而定期实施的检查测试，如内部控制有效性测试。

缺陷报告和整改在之后第4）点单独讲述。

2）测试检查

测试检查是指在内部控制日常监督检查的基础上，由有关部门或单位组织的对内部控制设计和执行的有效性进行的检查测试，并根据检查结果对内部控制的有效性做出评价。测试检查根据测试主体和测试范围及效力不同，分为管理层测试、专项测试、自测等。

① 管理层测试。《内控规范》要求对公司内部控制的有效性进行自我评价，披露年度自我评价报告。管理层测试是针对公司内部控制设计与运行的有效性，由公司管理层授权内审部门或者内部控制专门机构具体实施

的监督检查，并出具内部控制自我评价报告的过程。通过管理层测试，发现内部控制设计和执行有效性的缺陷，并按照缺陷认定标准，对控制缺陷进行分析和评价，确认一般缺陷、重要缺陷和重大缺陷，同时对有效性问题的整改情况进行跟进。

② 专项测试。专项测试是内部控制管理部门针对新建单位、管理薄弱环节、高风险领域和关键管理岗位进行的专题检查测试，或是在企业发展战略、组织结构、经营活动、业务流程、关键岗位员工等发生较大调整或变化的情况下，对内部控制的某一或者某些方面进行的有针对性的监督检查。例如，针对近年来发生过重大风险事件的业务，审计发现违规违纪案件的单位，对内部控制体系运行过程中容易出现控制缺陷的环节进行检查，对新建单位、新增业务、特殊风险业务的检查，对人、财、物管理部门有业务处置权的关键岗位的监督等。

专项测试主要是以风险为导向而组织的某业务领域的检查测试，一般没有固定的周期和时间规定，可以根据需要采取定期或不定期的检测。

③ 自测。自测是指下属公司的自我测试。它是由下属公司针对内部控制设计和运行的有效性，由下属公司管理层授权相关部门根据总部内部控制测试要求，具体实施检查并出具本公司内部控制自我评价报告的过程。下属公司根据总部的安排对内部控制执行情况进行自我测试和评价，并建立和保留完整、规范的测试记录文档。自我测试结束后，出具本单位内部控制的有效性声明。

下属自我测试参考管理层的方法和程序进行，但需要结合本单位的实际，考虑经营管理的薄弱环节，考虑自身的业务特点、风险变化等因素，与提升企业经营管理水平结合起来。

自我测试是执行内部控制监督检查机制的重要方式。为了保证自我测

试的效果，需要制定专门制度，明确谁是责任人、什么时间检查、检查的内容是什么、发现问题怎么整改、谁负责整改措施的验证，以及出现重大缺陷和重要缺陷谁负责、负什么责任、处罚措施是什么，等等。

3）外部审计

外部审计是指接受外部审计师对企业内部控制设计有效性和执行有效性的检查评价，并根据检查结果对内部控制有效性发表意见。

外部审计是独立于控制活动之外而采取的定期评估行为，是确保内部控制体系合法、合规运行的重要手段，是独立判断企业内部控制环境建设和业务控制的权威性措施，它在内部控制体系的运行过程中发挥着不可替代的作用。

测试的范围、方法、内容等，将在本书第6章详细介绍。

4）缺陷报告和整改

① 缺陷定义。缺陷是指在内部控制过程中，当某项控制的设计或运行不能使管理层或员工在正常行使其职责过程中及时防止或发现错报时，表明存在内部控制缺陷。缺陷按其影响程度不同可分为一般缺陷、重要缺陷和重大缺陷。

② 缺陷认定。根据上述的各项测试后，汇总发现的缺陷。依据缺陷认定标准，识别出一般缺陷、重要缺陷和重大缺陷。

缺陷的分类、认定标准、方法与程序等，将在本书第6章详细介绍。

③ 缺陷汇报。通过持续监督和独立评估获取的来源于内部认定和外部审计的缺陷，由内审部门或者专门的内部控制机构根据缺陷的性质和影响，按以下要求进行报告：

- 对于一般缺陷，向管理层汇报。
- 重要缺陷在认定后，向管理层和审计委员会汇报，必要时向董事会

汇报。

- 重大缺陷在认定后，向管理层、审计委员会和董事会汇报。

④ 缺陷整改。缺陷整改工作做得如何，对能否通过内部控制审计产生直接影响。

A．缺陷整改的责任。为了确保整改按时有效执行，明确缺陷整改责任主体是关键。

- 一般缺陷，由缺陷发现单位或部门自行整改。
- 重要缺陷，由缺陷发现单位或部门提出整改建议，包括整改时限，报内审部门或内部控制专门机构审核同意后实施。
- 重大缺陷，由内审部门或内部控制专门机构提出整改建议，包括整改时限，报管理层批准后实施。

内审部门或内部控制专门机构跟进缺陷整改工作，整改措施落实后经过一定时期的运行，进行跟进测试，评价整改是否有效。

B．缺陷整改特别关注事项。

- 舞弊事项。内部控制审计中，发现管理层的舞弊，即意味着内部控制无效。建立并完善反舞弊的内部控制，加强对反舞弊内部控制的监督检查，及时发现和纠正内部控制执行过程中的问题，通过积极的防控措施，从源头上预防舞弊的发生。
- 年末一次性完成的财务处理事项。主要是指财务报告流程。财务报告流程多为年度控制，即只在年末发生一次，发现缺陷则没有改进的空间和余地。如果不做提前考虑，不采取预防性措施，一旦测试发现问题，后果将难以挽回。因此，尽早查找执行中可能存在的问题，并在年末前使所发现的缺陷得到有效整改，确保这些年度财务报告流程的控制一次通过。

5.2 内部控制维护

《内控规范》第八条规定："企业应当建立内部控制实施的激励约束机制，将各责任单位和全体员工实施内部控制的情况纳入绩效考评体系，促进内部控制的有效实施。"内部控制涉及企业经营管理的全过程和各个环节，是一项由全体员工共同参与和实施的系统性工程。针对内部控制的这一特点，以人为本，建立权责明晰、奖惩结合的激励与约束机制，即责任机制与奖惩机制，确保内部控制体系持续有效运行。

1. 责任机制

内部控制责任机制是以内部控制组织体系为基础，旨在明确责任、落实责任、纠正过失，构建清晰、严明的工作责任环境，促进内部控制责任到位和执行能力提升的一整套制度、办法和运行程序。主要反映在以下几方面。

（1）明确责任主体

公司 CEO 和 CFO 就公司内部控制有效性发表声明，并对内部控制审计中发现的控制缺陷负责。

下属公司的 CEO 和 CFO 就本单位内部控制有效性发表声明，并对内部控制审计中发现的控制缺陷负责。

没有通过审计的单位，该单位的 CEO 和 CFO 承担主要责任。

（2）责任分解

公司 CEO 和 CFO 将内部控制责任横向、纵向进行分解，将责任逐级落实到总部职能部门及岗位和下属公司。

下属公司的 CEO 和 CFO 则将内部控制责任逐级分解到具体部门及岗位。

这样，整个公司的内部控制责任就层层分解到人，责任到人。

（3）责任追究

如果在内部控制测试检查中发现问题，按照缺陷级别落实相应人的责任。

① 发现导致内部控制失效的重要缺陷和重大缺陷或发生重大风险事件的，追究有关单位主要领导和相关人员的责任。

② 对发现的一般性缺陷，加强流程负责人的考核和培训。

③ 对关键岗位不能适应工作要求的人员，要及时调整工作岗位。

（4）需要注意的问题

① 责任定位的边界要清晰，不存在交叉，否则存在责任缺陷。

② 责任必须经过相应责任人确认，否则为无效责任。

③ 责任追究办法必须明示，为责任人所完整掌握，否则责任将失去约束力。

④ 责任问题核实后，追究责任必须依据办法坚决执行，否则影响责任机制的运行质量，或导致责任机制失效。

相关链接

单位（部门）负责人内部控制责任承诺书举例（摘要）

根据公司内部控制体系建设要求，确保全面通过外部审计。为做好本单位（部门）内部控制管理工作，本人向公司承诺：

- 认真开展内部控制体系文件的学习、培训和宣贯工作。在组织本单位（部门）全员学习内部控制体系的基础上，要让每名流程负责人知道做什么，怎么做，留下什么证据；知道哪些是关键控制，怎么控制；知道控制到了什么程度，达到什么标准。
- 单位（部门）领导是本单位（部门）内部控制第一责任人。督促

流程负责人按照内部控制要求实施，及时整改缺陷。

- 确保内部控制测试不出现控制缺陷。将责任分解到人，层层把关，落实责任。
- 如违反上述承诺，造成本单位（部门）发生控制缺陷，按照公司内部控制考核机制要求规定接受处罚。

承诺人：王华

2010年×月×日

2. 奖惩机制

内部控制奖惩机制是以考核为基础，通过利益手段驱动内部控制的有效执行。

内审部门或者内部控制专门机构根据管理层测试、专项测试、自测、外部审计、缺陷评估结果和日常工作考核情况，对公司各部门、下属公司内部控制体系运行情况进行评价，并编制公司内部控制评价报告，报管理层审核确认。

内部控制体系评价结果是公司管理层对公司各部门、下属公司高级管理人员进行业绩考核、实施奖惩的重要依据和参考。

把内部控制与风险管理体系建设和执行评价结果纳入高管人员考核和离任、责任审计中，并与职位晋升、薪酬分配挂钩，逐步构建支撑内部控制与风险管理体系持续运行的长效机制。

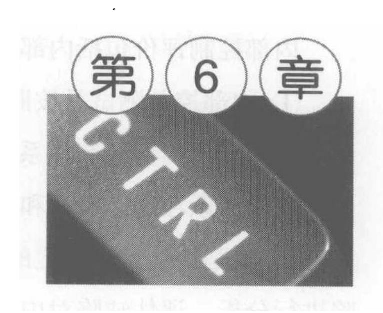
相关链接

奖惩条例举例（摘要）

- 被评价单位测试检查发现的问题，经过分析被认定为未构成缺陷的，被评价单位需根据整改建议的要求在规定时间内组织完

成整改。

- 被评价单位测试检查发现的问题，经过分析被认定为一般缺陷的，扣减被评价单位管理层薪酬5%。
- 被评价单位测试检查发现问题并被认定为重要缺陷的，扣减被评价单位管理层薪酬10%。
- 被评价单位测试检查发现问题并被认定为重大缺陷的，扣减被评价单位管理层薪酬30%。
- 被评价单位出现重要缺陷或重大缺陷的，除经济处罚外，给予被评价单位主要领导相应的行政处分，如通报批评、责成公开检讨、降职降薪和调整岗位等。



内部控制评价

内部控制评价是按照规定的程序、方法和标准，对已经建立和实施的内部控制体系，从设计有效性和执行有效性两个方面对内部控制有效性进行测试、评估和报告的过程。

内部控制评价包括内部控制测试、缺陷评估和评价报告等。

① 内部控制测试是按照规定的程序、方法和标准，针对财务报告控制目标，对公司内部控制体系设计有效性和执行有效性进行检查，旨在发现内部控制体系在设计层面和执行层面是否存在缺陷。

② 缺陷评估是以规定的程序、方法和标准，对内部控制测试发现的缺陷进行分析，评估缺陷对内部控制的影响程度的过程。

③ 评价报告是在测试和缺陷评估结果的基础上，根据公司对外披露和内部控制管理的不同需要，对内部控制有效性进行评价及报告的过程。

内部控制评价主要内容如图 6-1 所示。

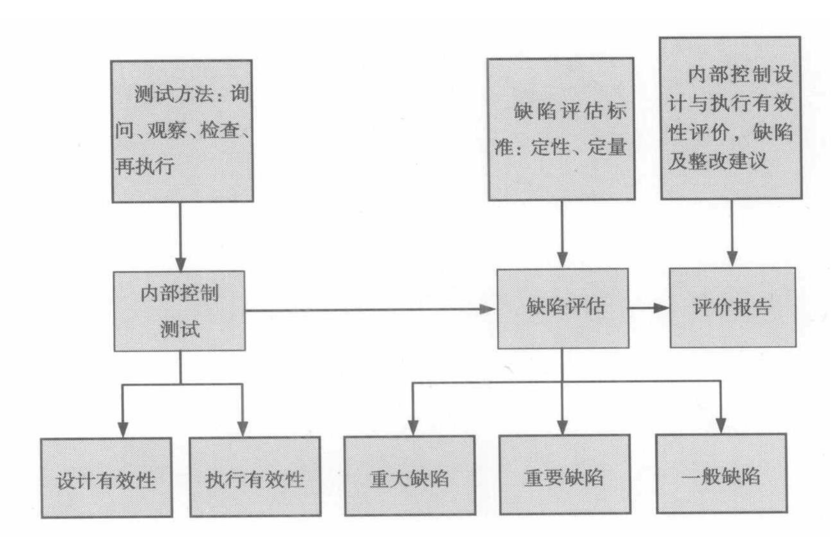


图 6-1　内部控制评价的主要内容

6.1 内部控制测试

6.1.1 内部控制测试概述

1. 内部控制测试的概念

内部控制测试是按照规定的程序、方法和标准，对公司内部控制体系设计有效性和执行有效性进行检查，查找内部控制设计和执行方面的问题，为内部控制体系有效性提供合理保证。测试主要包括以下内容：

① 根据设计和执行有效性评价的要求，对公司层面、业务活动层面和IT控制有效性分别进行测试。

② 对测试发现的缺陷进行评估并分类。

③ 根据测试结果，编制测试报告。

内部控制测试主要内容如图6-2所示。

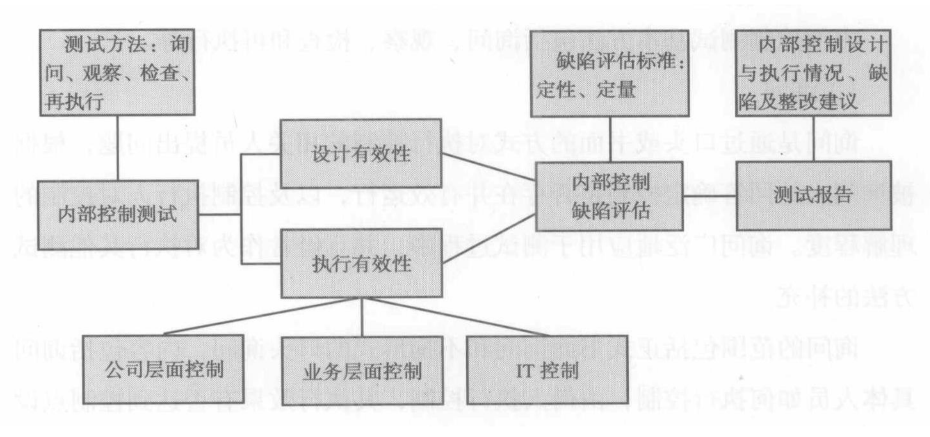


图6-2 内部控制测试的主要内容

2. 测试的分类

按照不同的标准有不同的分类，根据上述内部控制测试的概念，我们可以将内部控制测试分为设计有效性测试和执行有效性测试两种。

（1）设计有效性测试

设计有效性测试是通过一定的方法评价内部控制体系的设计是否能够有效地防范风险，为实现内部控制目标提供合理的保证，发现内部控制设计方面存在的问题，提出整改建议。

（2）执行有效性测试

执行有效性测试是通过一定的方法评价内部控制的运行是否按照内部控制设计执行，是否能够有效地控制风险，将风险控制到风险承受度内，发现内部控制运行方面存在的问题，提出整改建议。

3. 内部控制测试的方法

（1）测试方法

内部控制测试基本方法包括询问、观察、检查和再执行等。

1）询问

询问是通过口头或书面的方式对执行控制的相关人员提出问题，根据被询问人的回答确定控制是否存在并有效运行，以及控制执行人对控制的理解程度。询问广泛地应用于测试过程中，并且经常作为对执行其他测试方法的补充。

询问的范围包括正式书面询问和不拘形式的口头询问，内容包括询问具体人员如何执行控制，由何人执行控制，其执行效果有否达到控制点设计的目的。若在询问中发现问题，应判断问题是否会导致与报表相关的错报后果，以及如何解决有关问题。

在测试程序中，单独的“询问”不能为测试人员提供足够的证据来确定控制点执行的有效性，测试人员应结合其他的测试方法。

测试人员评估被询问者的反应是询问过程中的一个组成部分。被询问者的反应能提供测试人员可靠的信息，包括控制点执行人员的技巧和胜任能力，防止或查出错误或舞弊的控制点的敏感性，控制点能防止或查出错误或舞弊的频率等。当被询问者的反应给测试人员带来对控制点执行有效性的怀疑时，测试人员应执行额外的测试程序。

2）观察

观察是指测试人员对公司实物资产、有关业务活动的操作过程及其内部控制的执行情况等进行的实地察看，以了解控制的执行情况是否符合有关内部控制规定，是否与书面资料的记载相符。

例如，财务印鉴管理情况的检查，内部控制要求财务专用章和个人章分别由不同的人员进行保管，任何人不得保管 1 枚以上印鉴。测试人员可以让印鉴保管人员出示其负责保管的印章，观察不同印鉴是否由同一工作人员保管，以保证财务印鉴的管理符合控制要求。

又如，信息系统登录情况的检查，根据用户权限管理的规定，用户权限分配应遵循能够满足用户日常工作对系统资源的需求的最小授权原则进行授权。通过观察未授权人员账户登录是否会被系统拒绝，以保证系统的接触性控制是否存在。

但在采用现场观察法进行测试时，应充分考虑到测试人员不在现场时未按制度要求执行的可能性，因此，最好不要以一次观察的结果做结论，同时要结合其他的方法辅证现场观察的结果。

3）检查

检查是指测试人员检查与生产经营、财务活动的有关资料和控制点执

行的书面证据等。通过检查审阅文件资料，了解控制制度和流程，并证实该控制点已被执行。测试人员审阅的文件资料主要包括：以前的各种检查资料；被测试业务流程图；被测试流程说明或流程操作手册；有关会计资料、统计资料或其他核算资料；其他内部规章或管理制度；签字确认等有关的书面证据。

4）再执行

再执行是指测试人员根据控制点执行程序，依据风险大小抽取样本重新做一遍，并把重做结果与原有结果进行比较、分析数据，从而判断内部控制制度是否有效。如果处理后的新结果与原处理结果相同，则说明内部控制制度已发挥了其功能。

例如，在 IT 一般控制测试中，可以利用独立的数据进行复核测算，或者模拟系统的方式进行运算，输入假设的交易，用得到的结果与预计的结果进行比较来测试系统。

（2）举例

银行余额调节表测试，如表 6-1 所示。

表 6-1　测试方法举例

测试方法	测试内容
询问	询问准备及审阅银行余额调节表的人员是如何发现差异的，差异原因是什么，有什么样的步骤能确保相应的财务记录得到及时更正
观察	观察银行余额调节表准备的过程，并记录流程
检查	获取银行余额调节表，了解调节项目性质；追溯到相应的单据记录（如银行对账单）；检查调节表是否有相关负责人签字
再执行	比较某月银行对账单、账面余额及银行余额调节表，重新计算及查找差额，并追溯到相应的单据记录

（3）测试的可信度

不同的测试方法确信水平不一样，表 6-2 说明了不同测试方法的可信度。

表 6-2　不同测试方法的可信度

可信度	测试方法	特点
最不可能	询问	通过口头或书面形式确认控制存在
		最薄弱的测试方法
		应该与其他测试共同执行
		应该询问多人以确定结果一致
		文档记录要求：谁，什么时候，哪里，怎样
	观察	观察员工执行控制步骤
		可能需要其他跟进测试
		文档记录要求：谁，什么时候，观察的结果
	检查	获得资产存在证据的最简单的方法
		审阅文档记录或报告
		提供详细内容从而可以重复测试步骤并检验结果
	再执行	采用独立的数据重新进行对账
		按系统的计算公式重新计算
		在系统中输入测试数据来查看结果
最可能		测试文档记录的详细程度可以保证重新测试

6.1.2　测试的实施

内部控制测试分为设计有效性测试与执行有效性测试。内部控制设计有效性测试一般通过穿行测试来进行。本书第 4 章已经对穿行测试做了介绍，这里就不再累述。

根据本书第 3 章“合规范围”确定纳入范围的组织单位，所有关键控制都需要测试，包括公司层面、业务层面和 IT 控制。

1．公司层面的测试

根据第 4 章介绍的公司层面的内容，公司层面的测试范围包括内部环

境、风险评估、控制活动、信息与沟通、监督（包括反舞弊）五个方面，具体包括诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及审计委员会与监事会、组织结构、权利和责任的分配、人力资源政策与措施、员工胜任能力、反舞弊机制等内容。下面举例介绍其中几个方面内容的测试。

（1）诚信与道德价值观测试

公司制定《业务行为与道德守则》，审阅内容是否全面，是否符合国内外相关制度要求。

访谈公司员工，了解是否对《业务行为与道德守则》进行了宣传培训，了解员工对其的认知程度；通过检查相关培训记录等资料，确定公司是否对其进行了宣传和培训。

检查员工是否全部签署《业务行为与道德守则》并上报。同时通过访谈并对相关制度文件进行检查，了解并查看公司是否将职业道德标准包含在与客户及供货商的商业交往中，如将职业道德准则嵌入合同协议中，或者签署单独的协议等。

检查是否将《业务行为与道德守则》列入公司员工的培训内容，如通过员工培训，以及利用网络及其他形式进行《业务行为与道德守则》的学习与宣传。

是否对新员工开展关于职业道德规范方面的岗前教育培训，并在劳动合同中纳入遵守公司职业道德规范的内容。

（2）权利和责任分配测试

首先，获取公司相关授权权限方面的制度文件，如授权权限指引表，或者相关制度中规定的权限，如采购审批权限等。其次，选择部分管理人

员，审阅公司制度规定的相关权限描述是否与其岗位职责描述一致。再次，与相关部门负责人进行访谈，了解其是否定期对职责和权限进行审核，获得有关职责和授权的审批及变化的记录，审核其是否进行了适当的审批，并对变化进行了记录。最后，观察职责和授权有变化的员工的工作，是否按变化后的职责和授权执行。综合上述测试程序，判断责任和权力分配的适当性。

结合业务层面中对权限的测试，确认实际操作是否与制度规定的授权一致。

访谈人事部门负责人，并查阅职责和授权的审批及变化的记录，了解是否定期对权限指引表进行修订并记录，从而判断责任和权力分配的适当性。了解公司是否定期对岗位职责描述进行审核，如何审核。审阅相关资料，以确认公司定期对岗位职责描述进行了有效的审核。取得现任高级管理人员和重要部门相关岗位人员名单，选取财务人员、信息管理人员等数人，获得其岗位职责描述，确定描述是否包含以下要素：基本信息、岗位主要责任、工作职责（如清晰明确的监督职责和报告职责）、岗位权限、业绩指标、任职条件要求和工作环境等内容。询问了解其实际工作的职责和权限是否与岗位职责描述相一致。基于对公司组织结构及业务活动的理解，以及该岗位应具备知识技能和任职条件的职业判断，评价岗位职责描述内容的适当性，确保权利分配、职责分离的适当性。

结合 IT 控制测试中对财务、IT 人员权限测试的结果，确定其实际工作的职责和权限是否与岗位职责描述相一致，确认信息系统的责任和变化的授权是否适当。

下面是公司层面测试的一个例子，如表 6-3 所示。

表 6-3　公司层面测试举例——组织结构

内部控制关注要点	控制编号	负责人	控制描述	测试步骤	测试证据	缺陷	结论	整改计划
公司的组织结构能支持有效的财务报告内部控制	C100.01.8	管理层，投资者关系部	• 公司整体组织结构图依公司各下属公司间控股情况列置，且各子公司成立充分考虑需求 • 管理层根据公司经营状况评估公司的组织结构，当经营发生改变时，根据自身业务的发展状况，调整公司组织结构 • 投资者关系部每月更新公司组织结构图	（1）获取公司最新组织结构图，根据公司经营状况评估公司的组织结构，当经营发生改变时根据需要更新组织结构，以确保各下属公司的功能明确 （2）获取部门调整（新增或者裁撤）的任命、高管调整（任免、分工）的任命，查阅管理层设计合理的公司组织结构，以满足企业正常的运作	• 公司组织结构图 • 部门调整（新增或者裁撤）的任命 • 高管调整（任免、分工）的任命			

2．业务层面的测试

业务层面的测试，是指采用抽样测试的方法，对业务活动层面关键控制执行的有效性进行的检查，适用于手工控制、应用系统控制及电子表格控制测试。

（1）确定样本总量

样本总量是指测试对象。测试人员通过在样本总量中抽取样本和检查控制实施证据，来验证相关关键控制在样本总量中是否有效执行。

样本总量包括构成某类交易和事项的所有项目，测试人员应当确保样

本总量的适当性和完整性。适当性要求测试人员确定的样本总量应适合于特定测试目标。完整性要求测试人员应从样本总量项目内容和涉及时间等方面确定样本总量的完整性。

样本总量在大多数情况下并不是关键控制所对应的控制实施证据。

1）举例　有关费用报销的关键控制

关键控制：费用经办部门负责人、主管领导、财务总监，财务部门费用会计、出纳人员按照各自的职责权限分别对费用的原始凭证进行审核（原始凭证包括费用报销审批单）。

该关键控制的控制实施证据是费用报销审批单，但是针对该关键控制的测试样本总量不应该是全部的费用报销审批单。这是因为，如果以全部的费用报销审批单作为样本总量进行抽样，就不能发现已经入账但是没有适当的费用报销审批单的费用项目。所以针对该关键控制的测试样本总量应该是明细账中的全部费用项目，而不是费用报销审批单。

在该例子中，为了保证样本总量的完整性，关键控制测试对应的样本总量是全部的业务，但有的时候为了便于理解和操作，样本总量也可能是控制实施证据，即相关的表单。在这种情况下，测试步骤中就需要有保证样本总量完整性的相关步骤。

2）举例　有关计提坏账准备的关键控制

关键控制：每半年财务部门会同相关部门对应收款项进行全面检查，预计各项应收款项可能发生的坏账，确定坏账准备计提范围、计提方法和计提金额。

针对该关键控制进行测试，理论上说，样本总量应该是被测试单位的全部应收款项，但是这样抽取样本不便于理解和操作，所以可以把测试期间内全部的坏账准备检查测算表（控制实施证据）作为测试的样本总量。

如果这样，就应该包括如下的测试步骤：核对抽取的坏账准备检查测算表是否涵盖了全部应收、预付款项。

（2）样本的选取

1）抽样原则

样本选取的原则是能够代表样本总体。测试样本抽取原则应考虑的要素如下（但不限于）：

- 保证抽取样本时应包括各主要交易类型。
- 抽取价值大的交易类型比抽取价值小的频次较多。
- 若控制点在业务流程中采用系统自动控制，且存在良好的 IT 一般控制，最合适的测试方法是测试一个样本；若不存在良好的 IT 一般控制，则需按照人工控制的抽样方式选取样本量。

2）抽样方法

- 任意抽样。不存在如何选择性的抽样，可以在所有数据比较一致的情况下选用。例如，在 IT 系统中，电脑对数据的处理是一致的。（非统计学抽样）
- 随机抽样。随机抽样一般被认为是最具有代表性的取样方式。随机选取通常是采用电脑来完成的。（统计学抽样）
- 连续抽样。如果所有数据的总数是可知的，一个系统的抽样可能更合理，如抽取第 *n* 个数据为样本。（非统计学抽样）

例如，总数为 200，抽样数量为 9，则需要从每 22 个（200÷9=22）抽取一个样本。假定是从第 8 个开始，样本即为 8, 30, 52, 74, 96, 118, 140, 162, 184。

采用的抽样方法主要是依据所选取样本总量的形式而决定的，如样本总量为 1 000 张连续编号的发票，最佳的抽样方法为连续抽样。同时，在

制作测试计划时，我们也需要对选取抽样方法的原因进行描述。



如果所选的样本不能用做测试怎么办

- 例如，我们挑选尾数为 8 的发票作为控制测试的样本，发现其中一张是作废的发票，此时，我们可以挑选下一张发票作为替代的样本。选取替代样本，要详细记录选择替代样本的原因。
- 如根据以上的抽样方法无法找到一个替代样本，将无替代样本的情况作为差异记录下来，在下一轮测试中重点关注。

3）确认样本量

自动应用控制的样本量不考虑控制频率，固定为 1 个。

手工控制中定期发生的控制的样本量是通过控制发生的频率来确定的。

手工控制中不定期发生的控制或者执行对象比较多的定期发生的关键控制，需确定该控制在一个会计年度内大约发生的次数，折合成控制发生的频率后再确定样本量，样本数量的具体确定参照表 6-4。

表 6-4　样本量数量参考表

	发生次数	控制频率/折合频率	样本数量
自动应用控制		不适用	1
手工控制	1	每年	1
	2	每半年	2
	4	每季	2
	12	每月	4
	52	每周	10
	250	每日	30
	大于 250	每日多次	45

样本数量，要参考企业规模、业务复杂程度、具体控制点的风险水平等来确定。

不定期发生业务活动样本量和执行对象比较多的定期发生的控制样本量的确定举例。

① 不定期发生的控制样本。IT 系统用户变动的控制频率是随时的，测试人员需要询问被测试单位该控制负责人测试期间内用户变动数量，并与从人力资源部门取得的员工变动记录进行核对，然后推算全年员工变动数量，再参照表 6-3 确定应抽取的样本量。假如被测试单位 2010 年 1 ~ 3 月某 IT 系统共变动了 12 个用户，如果通过访谈得知用户变动在全年的分布是比较均衡的，则推算全年用户变动约为 48 个（12×4），折合频率为每周一次，相应确定的样本量应该是 10 个。

② 执行对象比较多的定期发生的控制样本。编制银行存款余额调节表的控制是每月定期进行的，但是由于银行存款余额调节表是针对每个银行账户编制的，所以该控制就不能简单地视为月度控制。针对该控制，需要确定被测试单位银行账户的数量，推算一个会计年度内编制银行存款余额调节表的次数，确定测试需要的样本量。假如某被测试单位共有 30 个银行账户，推算全年编制银行存款余额调节表的数量为 360 个，则折合频率为每日，相应确定的样本量应该是 45 个。

（3）检查样本

根据选定的样本，对样本进行检查。重点关注控制结果是否正确、控制过程是否有效、控制实施证据是否完整有效。确定描述的控制在实际工作中是否得到执行，执行中的控制在风险控制文档中是否得到描述，是否留下实施证据。

（4）记录抽样测试情况

测试完成后，根据测试结果在测试表中详细记录访谈结果，包括测试

步骤及发现、测试结论、缺陷及原因等内容。对于发现的缺陷，应该取得测试证据的复印件，并与测试记录进行索引。

除抽样检查外，还可结合观察、再执行等方法进行测试。

下面是业务层面（适用于手工控制、应用系统控制及电子表格控制）的一个例子，如表6-5所示。

表6-5 流程层面测试举例——客户信息管理（ERP）

关键控制				适用情况		测试步骤	样本总体	样本数量	测试证据	缺陷	结论	整改计划
关键控制编号	控制描述	控制方法	控制频率	总部	下属公司							
K106.01.01	在.ERP系统中对缺省客户信用额度进行合理配置,确保在系统内增加了新客户,信用的风险级别为预付款,信用额度默认值为0	自动	随时	不适用	适用	1．访谈关键用户，了解系统中关于缺省客户信用额度的配置情况 2．根据配置清单中"客户信用管理"流程的"K106.01.01"点，在系统中查看相应配置情况，确认是否与配置清单一致	配置清单					
K106.01.02	在ERP系统中进行合理配置,确保超过信用额度的销售订单或外向交货单被冻结，不能进行后续操作	自动	随时	不适用	适用	1．访谈关键用户，了解系统中关于超过信用额度后销售订单状态设置的配置情况 2．根据配置清单中"客户信用管理"流程的"K106.01.02"点，在系统中查看相应配置情况，确认是否与配置清单一致	配置清单					

3. IT 一般控制的测试

IT 一般控制是信息处理控制中的一种，是控制活动的内部控制组成要素的一部分。其中流程和程序用于对公司的信息技术活动和计算机环境进行管理和控制。通常分为信息技术控制环境、程序开发、程序变更、程序和数据存取（安全性）、计算机运行等多个领域。

通过 IT 一般控制测试，检查是否根据公司 IT 一般控制管理文件的要求，执行了信息系统管理的各项控制活动，从而提高应用系统控制的有效性，确保信息系统支持的应用控制是可靠的、生成的数据和报告是可信的。

（1）访谈

访谈执行控制的岗位人员，了解该业务人员是否真正理解所执行的控制，并对该业务人员的胜任能力做出判断，将访谈结果记录在测试表中。

IT 一般控制包括控制环境、信息安全、项目建设管理、系统变更管理、系统运行维护、最终用户操作等。

① 控制环境。包括 IT 一般控制环境、信息与沟通、风险评估、监控等。

② 信息安全。包括信息安全管理组织、逻辑安全、物理安全、网络安全、计算机病毒防护、第三方安全管理、信息安全事件响应等。

③ 项目建设管理。包括项目建设方法论、项目立项审批、商业软件与硬件的外购、项目启动、项目需求分析、项目设计、系统开发实施、系统测试、数据移植、系统上线、项目验收、用户培训和上线后评估等。

④ 系统变更管理。包括变更管理、日常变更流程、紧急变更流程等。

⑤ 系统运行维护。包括机房环境控制、系统日常运作监控、批处理作业调度管理、备份与恢复、问题管理等。

⑥ 最终用户操作。包括最终用户计算机操作安全制度、电子表格管理等。

（2）选取样本

结合访谈结果，确定样本总体和控制频率等问题，并选取样本。如果从测试起始时间到截止时间，由于业务发生量的限制，无法取得要求的样本量，则应该选取已有的全部样本，同时记录样本的选取情况，在备注中进行说明（样本量不足，要求××个，仅抽取了××个）。

在IT一般控制测试中，除了项目建设管理流程与信息安全领域采取全样本测试外，其他控制点测试需要的样本量其确定原则与关键控制抽样测试确定的原则相同。

在采用抽样检查的方法时，测试人员采用随意的方式选取样本，但是同时考虑以下两个因素：一是样本数量选取原则是测试业务发生期间随意选取，抽取样本时间分布均匀，随意选取是非统计抽样，不能集中抽取某一期间的样本，样本应分布在测试期间的不同时间段或时点，如每日的表格可抽取不同月份各一个，如1、3、5、7、9月各一个样本；二是常规业务样本与非常规业务样本的均匀分布，在测试时，样本对应的业务不能集中在一种类型，尽量覆盖所涉及的业务类型。

（3）检查样本

对样本进行检查，重点关注IT一般控制措施在实际工作中是否得到有效执行，是否符合IT一般控制措施的描述。

（4）记录抽样情况

记录测试过程，包括测试步骤及发现、测试结论、缺陷及原因等内容。对于发现的缺陷，应该取得测试证据的复印件，并与测试记录进行索引。

下面是IT一般控制的一个例子，如表6-6所示。

表6-6 IT一般控制测试举例——访问控制

关键控制				测试步骤	样本总体	样本数量	测试证据	缺陷	结论	整改计划
控制编号	控制描述	控制方法	控制频率							
K120.02.02	禁止操作系统管理员通过su命令获取oracle用户权限，从而能够进入数据库对业务数据进行直接访问；SAP系统信息安全管理负责人每月检查SAP服务器操作系统logon日志和su日志，对操作系统管理员通过su命令转换为数据库管理员的操作进行监控，调查发生这种情况的原因，确保数据库中的业务数据没有因为这种情况而受到不恰当的修改	手工	每月	1．访谈SAP系统信息安全管理负责人关于检查SAP服务器操作系统logon日志和su日志的管理情况 2．抽取3个月的logon日志和su日志检查记录（《SAP系统安全审计日志检查表》），检查是否填写了对日志所有记录的检查结果，是否记录了对异常情况的跟踪处理结果，是否有SAP系统信息安全管理负责人对检查结果的签字确认	全年的logon日志和su日志检查记录					

4．综合测试方法介绍

前文介绍了目前流行的一般测试方法，这些方法通常被称为传统的测试方法，主要是采用内部控制标准测试模板，根据业务发生的种类，按照一定的样本量随机抽取样本，通过样本使用的有效性来验证体系设计和执行的有效性。这种方法测试内容繁杂，但是很多时候，并不能发现问题，暴露出效率与效果不甚理想的问题。

选择适当的测试方法，对于发现问题、解决问题，以及提高企业管控能力非常重要。按照业务链条发展过程展开测试，更多的是借助审计的方法和技巧，甚至于借助职业判断来发现更深层次的执行层面的各种问题，我们称之为综合测试方法。以下是根据多年实务经验总结出来的几种方法，很多人都应该使用过，这里仅供参考。

（1）穿插法

穿插法是指在测试过程中，将相关的业务流程结合一起测试，还可以将公司层面与手工测试相结合，通过综合分析，发现在单一流程或单方面测试中不能发现的问题。

1）相关业务流程结合测试

相关业务流程结合在一起测试，可以发现相关业务链条的内在联系，规避单一流程测试时链条信息中断的情况发生。

例如，针对事后合同的问题，如果单纯在合同签订流程中进行检查，可能无法查出，因为事后合同在合同管理样本总体中是不存在的，总体中没有的样本是不会在测试中发现问题的。针对此情况，公司可以通过审阅采购流程，在取得全部的施工项目进度表的基础上抽取已实施或正在实施的项目，通过访谈了解项目执行情况后，再检查合同签订情况。凡是正在施工或已完成的项目，均应该签订施工合同。在合同主管部门取得项目主管部门签订的所有合同作为样本总体，将已抽取实施的项目与合同总体一一对照，即可查出是否为事后合同。

2）与公司层面测试相结合

与公司层面测试相结合，可以发现业务管理与授权管理及偏离职业道德导致风险失控等方面的问题。在公司层面测试中，着重关注投诉举报和违规处理、反舞弊等主题的测试结果。

例如，在查阅投诉举报信息及违规处理事项涉及的相关文件资料时，要考虑相关的业务流程执行是否准确。如果发现投诉举报记录中存在采购人员收受回扣的举报信息，在业务流程测试时应重点关注“采购流程”的设计与执行的有效性，以及反舞弊措施是否有效等。

又如，在测试高层基调、风险评估等主题时，通过与高管人员访谈，获得投资等方面信息，要重点关注预算的落实情况。通过访谈获得投资哪些项目，产生了哪些效益等，但测试人员在公司预算里面未找到该投资项目，针对此问题再进一步对投资支出等资料深查细究，就能发现预算外投资的问题。通过多个相关流程和多个主题穿插测试获得信息的相互借鉴，来发现单一流程或单个主题测试中较难发现的问题，多角度审视内部控制体系运行的有效性。

（2）倒查法

倒查法是根据业务链条发生的环节，分析并寻找业务链的特点，发现其内在联系，从业务链末端或下游业务入手，发现问题后进行反查的一种方法。该方法适用于采用正查法无法查出问题或无法获取所需样本的情况。

例如，在测试材料采购流程时，重点关注采购计划和采购合同的有效性。如果用正查法测试，先从系统中查阅某批物资的采购计划、采购合同、入库验收单、出库单，最后到财务入账等手续，可能无法直接查出问题，这时要考虑采用倒查法，如图 6-3 所示。

（3）IT 与手工结合法

内部控制体系有效运行离不开信息系统的支持，为确保企业所使用的应用系统的安全完整，防范欺诈和舞弊行为，就要对应用系统应用管理进行定期检查，其中对权限的检查尤为重要，同时信息与手工测试要有关联性。

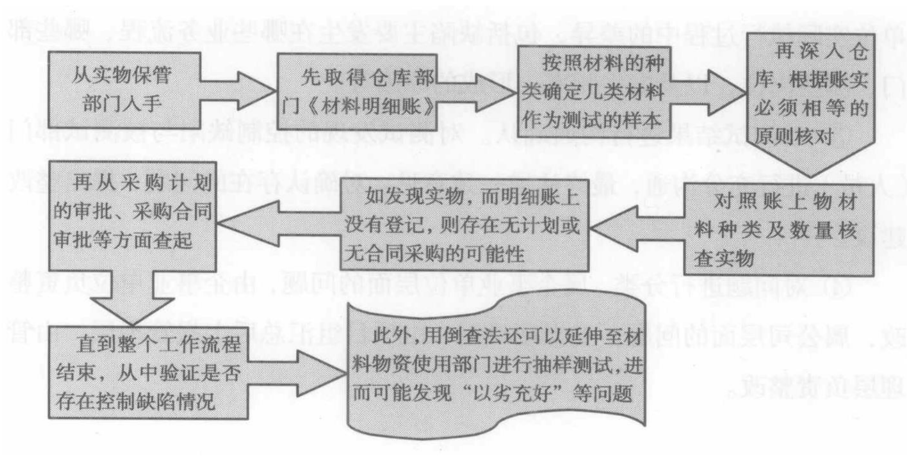


图 6-3　倒查法举例

例如，在手工测试查阅记账凭证时，有审批的痕迹，但这个审批是否有效，可通过权限测试来确定。通过权限测试，一方面可发现多余权限，另一方面可发现审批人所分配的权限是否符合不相容岗位原则和权限最小原则，这样可规避由于不应有的权限人进行审批导致舞弊风险的产生。

另外，通过电子表格测试可发现因手工测试不能发现的公式变更而导致的数据不准确等风险的产生。所以，信息系统测试与手工测试的有机结合可规避许多手工测试不易发现的问题。

6.1.3　测试报告

1．测试总结

① 汇总整理相关测试记录，测试人员汇总全部控制缺陷，并归档相关实施证据。

② 测试人员汇总发现的问题，对测试结果进行分析，包括分析被测试

单位实际执行过程中的差异，包括缺陷主要发生在哪些业务流程、哪些部门、哪些岗位，以及发生频率、形成的原因等。

③ 对测试结果进行沟通确认。对测试发现的控制缺陷与被测试部门（人员）进行充分沟通，最终达成一致意见。对确认存在的问题，提出整改建议。

④ 对问题进行分类，属企事业单位层面的问题，由企事业单位负责整改，属公司层面的问题，上报项目组，由项目组汇总后上报管理层，由管理层负责整改。

2. 测试报告

测试报告主要包括以下几个方面的内容：

① 内部控制体系运行情况。测试单位内部控制设计与执行有效性总体评价，简要叙述内部控制机构设置情况、公司流程和控制的重大变化情况及缺陷整改情况等。

② 测试发现与缺陷说明。首先说明控制缺陷总体情况，然后按照公司层面、业务活动层面和信息系统层面分别对重要控制缺陷进行说明。

③ 整改意见及建议。针对测试发现的控制缺陷，提出建议和措施。

6.2 缺陷评估

6.2.1 缺陷评估概述

1. 缺陷评估的概念

缺陷评估是以一定的方法和标准，对内部控制存在的设计和执行有效

性方面的问题进行分析，进而评估内部控制缺陷的影响程度及发生可能性的过程。

缺陷评估高度依赖于评估人员的职业判断，因此对评估人员的经验和能力都有较高的要求。

缺陷评估采用定量判断和定性分析相结合的方法。以测试发现的控制缺陷为基础，将缺陷评估分为缺陷确认、单个缺陷评估、缺陷汇总评估三个阶段。

2．缺陷评估的目的

缺陷评估的目的是评价在设计层面和执行层面是否存在控制缺陷及缺陷的影响程度，以作为管理层发布内部控制自我评估报告的依据。

3．缺陷的分类

缺陷的分类可以有以下两种方式。

1）按严重程度分

企业应当对内部控制缺陷进行综合判断，按其严重程度分为重大缺陷、重要缺陷和一般缺陷。

① 重大缺陷是指一个或多个控制缺陷的组合，可能导致企业严重偏离控制目标的情形。

② 重要缺陷是指一个或多个控制缺陷的组合，其严重程度和经济后果低于重大缺陷，但仍有可能导致企业偏离控制目标的情形。

③ 一般缺陷是指除重大缺陷、重要缺陷之外的其他控制缺陷。

2）按测试过程分

① 设计缺陷。缺少实现控制目标所需的控制，或者现有控制没有得到

合理的设计，即使按照设计的控制运行，也无法实现控制目标，则为设计缺陷。

例如，由出纳人员执行银行对账工作，虽然该项关键控制在实际中得到执行，但由于是不相容岗位，属于不相容岗位未进行分离，属于设计缺陷。

② 执行缺陷。如果一个设计适当的控制未按照设计运行，或者执行人员没有适当的授权或能力有效运行该控制，则为执行缺陷。

例 1：内部控制文档中的控制措施设计描述为“合同要经过财务、技术、法律三项审查，才能报主管领导审批”。如果没有严格执行此规定，则反映了内部控制文档所描述的控制在实际中没有执行，属于执行缺陷。

例 2：月末，财务与相关部门账账核对、账实核对，核对不一致时未能及时查明原因并处理，造成作业步骤不完整，也属于执行缺陷。

例 3：在核对往来时，本来双方金额不一致，但因为工作疏忽误以为一致，造成控制无效。

6.2.2 缺陷评估认定标准

1．重大缺陷认定标准

重大缺陷的认定要从定量和定性两方面综合判断。

（1）定量标准

1）针对单个控制

定量首先要确定重要性水平和一般性水平，《企业内部控制审计指引》第二十条规定：“在计划内部控制审计工作时，注册会计师应当使用与财务报表审计相同的重要性水平。”

一般情况下，采用合并报表税前利润的5%和1%分别作为重要性水平标准和一般性水平标准：影响水平达到或超过当年公司合并报表重要性水平，即税前利润的5%，直接认定为重大缺陷；影响水平低于公司合并报表税前利润的5%，但达到或者超过1%的，经过定性因素分析，认定为重要缺陷。

2）多个控制缺陷的组合

在对公司缺陷进行认定时，多个控制缺陷影响同一个目标，应该放在一起考虑。

影响水平达到或者超过当年公司合并报表税前利润的5%，认定为重大缺陷；影响水平低于公司合并报表税前利润的5%，经过定性因素分析，认定为重要缺陷。例如，管理费用会计科目中，各单位测试中发现的缺陷影响水平均小于单个单位重要性水平，但汇总各单位缺陷影响程度大于公司合并报表税前利润的5%，该控制仍然存在重大缺陷。

与IT一般控制缺陷有关或者由它所引起的应用系统控制缺陷，在进行上述定量分析后，如果超过 5%，或者虽不超过公司合并报表税前利润的5%，但经过定性因素分析也可被确认为重大缺陷，如图6-4所示。

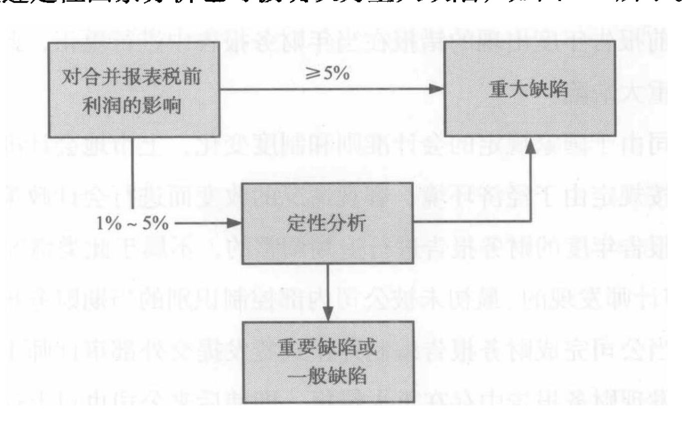


图6-4　重大缺陷认定标准



（2）定性标准

《企业内部控制审计指引》第六十九条规定："下列迹象可能表明内部控制存在重大缺陷：

（一）注册会计师发现高级管理人员舞弊；

（二）企业重述以前公布的财务报表，以更正重大错报；

（三）注册会计师发现当期财务报表存在重大错报，而控制未能发现；

（四）审计委员会对财务报告及内部控制的监督无效。"

定性标准，主要是下面几条。

① 识别出高级管理层中的任何程度的舞弊行为。由于高层基调在整个控制环境中的重要作用，高级管理层的任何程度舞弊都会对控制环境产生消极影响，所以与财务报告相关的高级管理层人员任何程度的舞弊行为都会造成重大缺陷。

② 对已签发的财务报告进行重报以反映对错报的更正。公司按规定期限报送已签发的财务报告（含年报和半年报）后，如果公司对财务报告重新报送以更正财务报告中的错报，包括对报告年度财务报告错报进行更正重报和以前报告年度出现的错报在当年财务报告中进行更正，此类情况可认定存在重大缺陷。

但公司由于国家规定的会计准则和制度变化，上市地会计准则变化，以及公司按规定由于经济环境、客观情况的改变而进行会计政策调整，需要对以前报告年度的财务报告进行追溯调整的，不属于此类情况。

③ 审计师发现的、最初未被公司内部控制识别的当期财务报告中的重大错报。当公司完成财务报告编制并正式签发提交外部审计师审计后，外部审计师发现财务报告中存在重大错报，即使后来公司也对上述重大错报进行了更正并重新编制了财务报告，仍属于存在重大缺陷。

④ 审计委员会对公司的对外财务报告和财务报告内部控制监督无效。监管机构对审计委员会有明确的职责和资质要求，如果审计委员会不能履行对公司的对外财务报告和内部控制实施有效的监督或不具备监督的资质及能力，就可以确认审计委员会的监督无效。

A. 审计委员会的有效监督

审计委员会章程和程序涵盖审计委员会主要的角色和责任。

单独与首席财务官、会计人员、内部审计师和外部审计师会面的频率和时间，以讨论财务报告流程、内部控制与企业风险管理体系，以及管理层绩效的合理性等提出重大意见和建议。

审计委员会活动的书面证据应充分。

B. 独立性

审计委员会的所有成员均应是董事会的成员，并且具备独立性。

审计委员会成员不能收受该上市公司的任何咨询费、顾问费或其他补偿性费用，不能是该上市公司或其子公司的关联人员。

C. 财务专家

审计委员会的成员中至少有一名财务专家。

D. 反舞弊控制

监督管理层反舞弊控制程序的关键内容，包括以下几点：参与定期的舞弊风险评估工作；审核管理层针对已识别的舞弊风险采取的应对措施；取得通过举报机制获知的问题的报告；取得管理层、内部或外部审计师发现的舞弊事件的正式报告；参与重大舞弊事件或有关财务人员舞弊事件的调查。

E. 审计委员会的角色和责任

监督公司的内部审计职能，包括以下几点：任命内部审计主管前，事先征求审计委员会意见；审核年度内部审计预算和计划，审核内部审计的

重要报告或重大发现；每年至少同内部和外部审计师单独会晤一次；必要时召开临时会议。

F．监督财务报告流程

审计委员会获得充分的信息以审核财务报告和其他公开财务报告的合理性。

审计委员会与高级管理层和外部审计师讨论财务报表及财务报表附注的内容。

审计委员会成员具备必要的经验以审核公布的财务信息，并与管理层和审计师进行讨论。

审计委员会及时审核中期和年度财务报告、其他报告和新闻公告。批准或建议董事会通过有关的报告。

与管理层和内外部审计师充分讨论重要事项，包括重大会计政策、判断性的会计估计等。

G．监督有关财务报告的内部控制

讨论管理层发现的所有重要缺陷和重大缺陷，并审核相关的披露事项。

如果审计委员会一个或所有成员都不能满足"财务专家"的要求，说明审计委员会不具备监督财务报告的能力和经验，可以确认审计委员会监督无效；如在其他方面不能履行监督职责，综合考虑也会导致对外财务报告和财务报告的内部控制无法实施有效监督，也可以确认审计委员会监督无效。

2．重要缺陷认定标准

（1）定量标准

1）单个控制

影响水平低于5%，但是达到或超过1%，直接认定为重要缺陷；影响水

平低于 1%的，经过定性因素分析，也可以认定为重要缺陷，如图 6-5 所示。

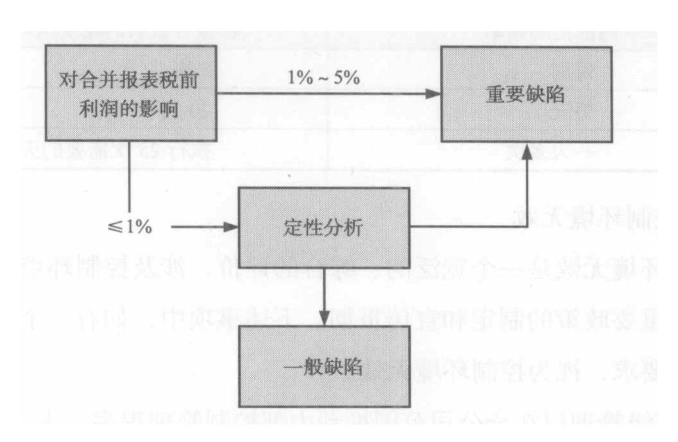


图 6-5 重要缺陷认定标准

2）多个控制缺陷的组合

与重大缺陷的认定标准相同，在对公司缺陷进行认定时，多个控制缺陷影响同一个目标，应该放在一起考虑。

影响水平达到或超过 1%，可以认定为重要缺陷；影响水平不超过 1%，经过定性因素分析，也可能认定为重要缺陷。

（2）定性标准

1）沟通后的重要缺陷没有在合理的期间得到纠正

外部审计发现的重要缺陷，在与管理层、审计委员会沟通后，公司没有及时整改或整改后没有充足的时间满足确认该缺陷纠正后是控制有效的。具体见表 6-7 内部控制有效运行的执行周期。

表 6-7 内部控制有效运行的执行周期

内部控制频率	在报告日前的建议执行时期
每季	2 个季度
每月	2 个月

续表

内部控制频率	在报告日前的建议执行时期
每周	5 周
每天	20 天
一天多次	执行 25 次需要的天数

2）控制环境无效

控制环境无效是一个宽泛的、综合的评价，涉及控制环境所有要素及管理层对重要政策的制定和宣传贯彻。下述事项中，如有一个或者一个以上不符合要求，视为控制环境无效。

① 高级管理层在全公司范围推动内部控制管理程序，主要内容包括：

- 建立公司治理结构，明确规定董事会、审计委员会、高管、业务单位领导、业务具体负责人、内部审计等职责。
- 公司的制度和政策必须在全公司得到贯彻执行。
- 建立全面的内部控制文档记录，并对内部控制体系的实施及持续维护进行监督。
- 实施定期评估，确保有关财务报告的内部控制在全年持续有效运行。对缺陷进行整改，并及时更新相关文档记录。

② 会计政策和程序。管理层应建立适当机制以获得会计准则的变化，以及其他涉及财务报告要求的法规的更新。主要内容包括：

- 编制会计政策手册，向各级管理人员传达并严格遵守。
- 定期审核和更新会计政策，如发生重大变更，应由高级管理层审批，并报审计委员会复核。
- 管理层与外部审计师和其他外部专家密切沟通，以理解和应对公认会计准则的复杂变更。
- 开展正式的培训和/或沟通以保证贯彻落实政策和程序。

③ 针对非常规、复杂或特殊交易的账务处理的控制。管理层建立政策和程序以识别和正确记录重要的非常规交易，主要内容包括：

- 管理层及时发现可能对财务报告造成重大影响的非常规交易、复杂交易或者特殊交易。
- 管理层采取适当措施，如会议讨论、咨询、调查分析等形式，对正确的会计处理达成共识，并恰当记录该决策过程。
- 就对财务报告造成重大影响的非常规交易、复杂交易或特殊交易，管理层与外部审计师进行充分讨论并进行适当的披露。

3）公司内部审计职能和风险评估职能无效

内部审计应当做到：制定内部审计制度，包括目标、工作范围、义务、独立性、职责、权利及审计实务标准等；与业务部门沟通；通过审计委员会审议；报高管层批准。

保持独立性。公司内审部门定期或应要求向监事会、董事会、审计委员会、管理层及时报告重要审计发现并提出处理意见；审计机构不承担本单位的经营责任，审计人员不执行生产经营管理业务工作的具体操作。

组织结构和人员资历。内审部门具备必要技能、相关经验及专业资格的内审人员，来完成规定的内部审计工作；接受继续教育和培训，保持胜任工作的知识、技能和其他能力。

4）对于非常规、复杂或特殊交易的账务处理的控制

非常规、复杂或特殊交易主要是非货币性交易、债务重组、外币业务、复杂交易等。会计核算人员或报表编制人员在处理上述业务时，如果难以进行职业判断，应逐级向上一级财务负责人报告，确定处理方法。

5）反舞弊程序和控制

公司必须实施“反舞弊控制”，涉及建立必要的程序和控制，通过宣传

培训使员工和管理层理解反舞弊控制，加强监督保证实施有效并不断持续维护等内容。如果公司在以下每个方面没有建立必要的控制和不能保证实施有效，都会造成重要缺陷的存在。

① 建立并有效执行职业道德规范。

职业道德应适用于所有负责会计或监管财务报告的员工，并清楚定义舞弊行为，说明应遵守的准则，建立确定违规行为的公正程序。

董事会和审计委员会应监管职业道德规范的执行，员工在雇用时及之后应定期接受职业道德规范的培训。

如果公司没有建立经董事会或有效运行的审计委员会审核的书面职业道德规范，即为重要缺陷。

② 建立投诉举报机制。内审部门建立道德热线或举报机制，为员工和其他人员提供报告可能违反道德准则的行为和舞弊事项的途径；审计委员会依赖现有投诉举报机制，通过对其的监督及接受定期汇报来完成其受理投诉的责任；每季度由审计部负责统一汇报公司所收到的关于会计、内部财务控制或审计方面的举报及处置情况。

如果缺乏这种举报及报告机制，将导致财务报告内部控制出现重要缺陷。

③ 审计委员会和董事会的监督。在公司章程或者相关制度中，应规定审计委员会和董事会系统地定期复核管理层建立的财务报告体系。董事会和审计委员会应积极监管舞弊行为。

如果审计委员会对反舞弊采取消极态度，则存在重要缺陷。

④ 调查与补救措施。管理层、审计委员会和董事会应采取恰当的措施，指出和披露内部控制存在的重大缺陷和重大缺陷、重大的实质性舞弊行为

及高层参与的任何程度的舞弊，并采取恰当的补救措施。

如果公司不向外部审计师或审计委员会披露关于重要缺陷或舞弊行为的信息，公司对认定的重要缺陷及已发现舞弊或疑似舞弊采取恰当的补救措施，都可确认为重要缺陷。

⑤ 控制措施。管理层应设计必要的控制措施以应付预见的舞弊风险，并予以记录。

如果没有必要的控制措施，或控制措施没有被有效执行来规避舞弊风险，则存在着重要缺陷。

⑥ 对于期末财务报告过程的控制。交易总数过入总账，初始、授权、记录和总账中账务处理，以及之中伴随的 IT 控制。

3．一般缺陷认定标准

在定量和定性考虑后，不属于重大缺陷和重要缺陷的，确认为一般缺陷。

6.2.3 缺陷评估程序

缺陷评估程序以测试发现的控制缺陷为基础，其程序如图 6-6 所示。

1．控制缺陷分析阶段

对控制缺陷进行汇总整理，纳入缺陷评估的是未整改或已整改但未达到合理运行时间的控制缺陷。

与测试人员及流程负责人进行必要的沟通，对控制缺陷的发生原因及未整改原因进行分析。

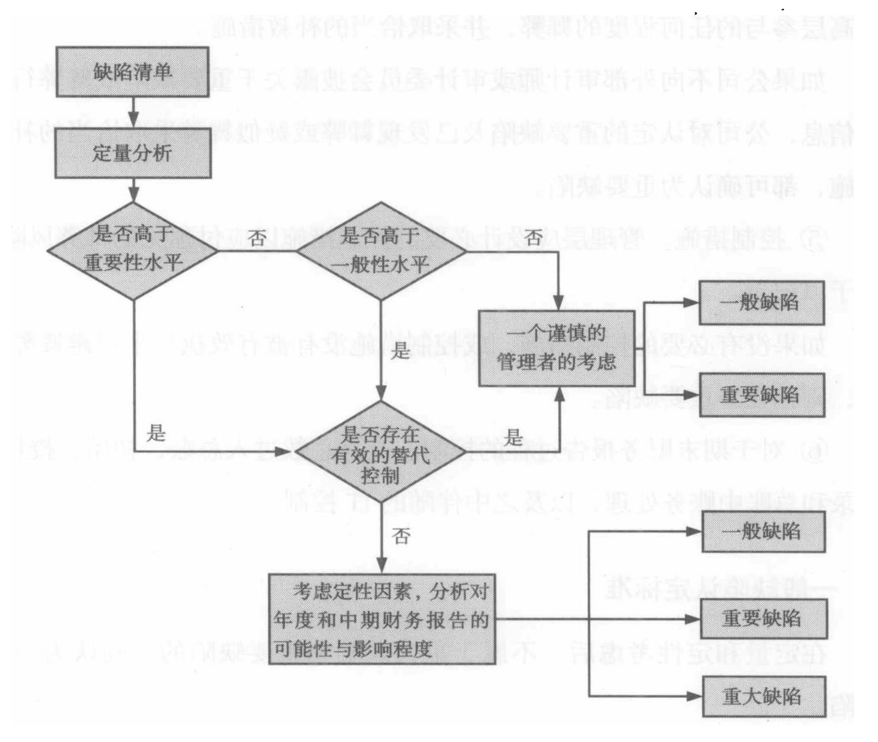


图 6-6　缺陷评估程序

2. 缺陷评估阶段

（1）定量判断

影响高于重要性水平，且不存在有效的替代控制，直接认定为重大缺陷。

（2）重大缺陷分析

对于影响水平大于重要性水平的控制缺陷，判断是否存在有效的替代控制，再进行定性分析。考虑可能性和影响程度等因素后，如果一个谨慎的管理者认为该控制缺陷影响高于重要性水平，则该控制缺陷确认为重大

缺陷。

替代控制考虑因素：如果存在替代控制且经测试控制有效，重新进行定量判断，确定缺陷类别，如降低缺陷类别；如果经测试替代控制无效，则不需要考虑替代控制。

（3）重要缺陷分析

对于影响水平大于一般性水平但小于重要性水平的控制缺陷，判断是否存在有效的替代控制，再进行定性分析。考虑可能性和影响程度等因素后，如果一个谨慎的管理者认为该控制缺陷影响水平低于重大缺陷造成的影响，但足以引起注意，该控制缺陷确认为重要缺陷。

替代控制考虑因素：如果存在替代控制且经测试控制有效，重新进行定量判断，确定缺陷类别，如降低缺陷类别；如果经测试替代控制无效，则不需要考虑替代控制。

（4）一般缺陷分析

对于影响水平小于一般性水平的控制缺陷，如果一个谨慎的管理者认为其影响水平低于重要缺陷造成的影响，但也应引起公司关注，则该控制缺陷确认为一般缺陷。

影响水平小于一般性水平的控制缺陷，不需要考虑替代控制。

3. 缺陷评估程序举例

某公司缺陷评估的重要性水平为 500 000 元，一般性水平为 100 000 元。

控制活动：每月编制银行存款余额调节表。

总体影响水平：银行存款收支全年大约为 40 000 000 元。

测试步骤：选择两个月，每个月选择 5 个银行账户，检查是否每个银行账户都编制了调节表，并且及时地调查和解决了所有非正常项目。

测试结果：两张调节表存在问题，测试人员发现 750 000 元的重大调节项目，而且已经存在一年以上。

1）判断是否为重要缺陷

总体影响水平为 40 000 000 元，大于一般性水平（100 000 元）；

替代控制：财务经理复核并在银行余额调节表上签字。因为财务经理没有发现上述的重大差异，此替代控制是无效的。

因此判定为重要缺陷。

2）判断是否存在重大缺陷

总体影响水平（40 000 000 元），超过重要性水平（500 000 元）。

因此判定为重大缺陷。

4. 缺陷评估结果对审计报告的影响

缺陷评估结果对审计报告的影响如表 6-8 所示。

表 6-8 缺陷评估结果对审计报告的影响

缺陷类型	与管理层沟通	与审计委员会沟通	与董事会沟通	公司对外披露	审计报告意见
一般缺陷	√				无保留意见
重要缺陷	√	√	√		无保留意见
重大缺陷	√	√	√	√	否定意见

6.3 评价报告

内部控制评估报告是公司根据内部控制测试及缺陷评估的结果，对公司内部控制有效性做出评价。

1. 管理层内部控制评估报告要素构成

内部控制评价报告至少应当包括下列内容：

① 组织实施内部控制评价的总体情况。

② 内部控制责任主体的声明。

③ 内部控制评价的范围和内容。

④ 内部控制评价的标准和依据。

⑤ 内部控制评价的程序和方法。

⑥ 内部控制重大缺陷及其认定情况。

⑦ 内部控制重大缺陷的整改措施及责任追究情况。

⑧ 内部控制有效性的结论。

存在一个或多个内部控制重大缺陷的，应当做出内部控制无效的结论。

2. 编制与披露程序

编制与披露程序如下：

① 收集相关信息，包括监管要求、法律法规要求、上年度的披露事项和内部控制缺陷评估结果。

② 内审部门或专门的内部控制机构编制管理层自我评估报告初稿，并由主管领导审阅。

③ 与律师和外部审计师进行沟通，根据其意见修改报告。

④ 内审部门或专门的内部控制机构领导审核报告，根据沟通及审核意见进一步修改报告。

⑤ 公司 CFO 审核管理层自我评估报告。

⑥ 提交董事会审定后，对外发布。

3．报告模板

下面是2009年万科企业股份有限公司内部控制自我评价报告。

万科企业股份有限公司
2009年内部控制自我评价报告

董事会声明

本公司全体董事、监事及高级管理人员承诺内部控制自我评价报告不存在任何虚假、误导性陈述或重大遗漏，并保证所披露信息的真实、准确与完整。

一、综述

在董事会、管理层及全体员工的共同努力下，本公司已经建立起一套比较完整且运行有效的内部控制体系，从公司治理层面到各业务流程层面均建立了系统的内部控制制度及必要的内部监督机制，为本公司经营管理的合法合规、资产安全、财务报告及相关信息的真实完整提供了合理保障。

2009年度，本公司参照财政部等五部委联合发布的《企业内部控制基本规范》及深交所《上市公司内部控制指引》等相关规定，坚持以风险导向为原则，对公司的内控体系进行持续的改进及优化，以适应不断变化的外部环境及内部管理的要求。

本年度，公司建立了覆盖总部、各控股公司及各业务部门的三级自我评估体系，组织总部及各控股公司对内控设计及执行情况进行了系统的自我评价。并通过风险检查，内部审计等对公司内部控制的设计及运行的总体情况进行了独立评价，具体评价结果阐述如下。

二、内部环境

1．治理结构

公司按照《公司法》《证券法》等法律、行政法规、部门规章的要求，建立了规范的公司治理结构和议事规则，明确决策、执行、监督等方面的职责权限，形成了科学有效的职责分工和制衡机制。股东大会、董事会、监事会分别按其职责行使决策权、执行权和监督权。股东大会享有法律法规和公司章程规定的合法权利，依法行使公司经营方针、筹资、投资、利润分配等重大事项的表决权。董事会对股东大会负责，依法行使企业的经营决策权。董事会建立了审计、薪酬与提名、投资与决策三个专业委员会，提高董事会运作效率。董事会11名董事中，有4名独立董事。独立董事担任各个专业委员会的召集人，涉及专业的事项首先要经过专业委员会通过然后才提交董事会审议，以利于独立董事更好地发挥作用。监事会对股东大会负责，除了通常的对公司财务和高管履职情况进行检查监督外，还组织了对控股公司的项目巡视，加强对各控股公司业务监督。经理层负责组织实施股东大会、董事会决议事项，主持企业日常经营管理工作。

公司与第一大股东及其关联企业在业务、人员、资产、机构及财务等方面始终完全分开，保证了公司具有独立完整的业务及自主经营能力。

2．机构设置及权责分配

公司结合自身业务特点和内部控制要求设置内部机构，明确职责权限，将权利与责任落实到各责任单位。

董事会负责内部控制的建立健全和有效实施。董事会下设立审计委员会，审计委员会负责审查企业内部控制，监督内部控制的有效实施和内部控制自我评价情况，指导及协调内部审计及其他相关事宜等。监事会对董事会建立与实施内部控制进行监督。经理层负责组织领导企业内部控制的

日常运行。

公司总部设立风险管理部具体负责组织协调内部控制的建立、实施及完善等日常工作，通过编制内部控制评估表，组织总部、各控股公司、各业务部门进行自我评估及定期检查，推进内控体系的建立健全。总部各专业部门及各控股公司均设有内控专员等相关内控管理岗位，负责本单位内部控制的日常管理工作。

3．内部审计

公司审计部直接向董事会审计委员会汇报工作，其负责人由董事会任命，保证了审计部机构设置、人员配备和工作的独立性。

审计部年初制定年度审计计划及工作程序，通过执行综合审计或专项审计业务，对公司内部控制设计及运行的有效性进行监督检查。对在审计中发现的内部控制缺陷，依据缺陷性质按照既定的汇报程序向管理层或审计委员会及监事会报告。

4．人力资源政策

人才是万科的资本，公司制定和实施有利于企业可持续发展的人力资源政策，将职业道德修养和专业胜任能力作为选拔和聘用员工的重要标准，切实加强员工培训和继续教育，不断提升员工素质。

《万科职员手册》明确了以德为先原则，是否具备良好的职业道德，是万科判断人才的首要标准。人力资源部制定各岗位的职位说明书，明确了每个岗位的职责和权限。定期进行专业人员的专业化考试，建立轮岗、交流机制，培养专业人员全面的知识和技能。每年人力资源部制定相关培训计划，组织具体培训活动。

公司还建立了全体员工的利益冲突申报制度，关键岗位员工强制休假制度和岗位轮换制度，以加强员工的自律及防止舞弊行为的发生。

5．企业文化

公司的核心价值观“创造健康丰盛的人生”包含“客户是我们永远的伙伴”、“人才是万科的资本”、“阳光照亮的体制”及“持续的增长和领跑”等理念。在坚持核心价值观的前提下，公司按照现代企业制度建立起了一套经营管理规范和流程。公司高度重视企业文化的宣传和推广，每年组织全公司范围内的“目标与行动”专题活动，由公司管理层进行公司目标和价值观的宣讲并要求所有员工签署受训确认书。在任用和选拔优秀人才时，一贯坚持“德才兼备、以德为先”的原则，把持续培养专业化、富有激情和创造力的职业经理队伍作为公司创立和发展的一项重要使命。

三、风险评估

为促进公司持续、健康、稳定发展，实现经营目标，公司根据既定的发展策略，结合不同发展阶段和业务拓展情况，全面系统持续地收集相关信息，及时进行风险评估，动态进行风险识别和风险分析，并相应调整风险应对策略。

公司由相关部门负责对经济形势、产业政策、市场竞争、资源供给等外部风险因素以及财务状况、资金状况、资产管理、运营管理等内部风险因素进行收集研究，并采用定量及定性相结合的方法进行风险分析及评估，为管理层制订风险应对策略提供依据。

2009年度，面对宏观环境、行业走向、竞争态势的种种不确定性和新的挑战，公司注重提升企业的专业能力，促进公司的发展由规模速度型向质量效益型转变，采取了项目获取坚持“精挑细选，把握机会”；开展成本对标，提高集中采购度水平，严格控制成本；实行费用预算硬约束和严格监督，降低费用水平；存货管理坚持“量出为入”的策略，以及积极拓展融资渠道等风险应对措施，以提升为股东持续创造价值的能力。

四、控制活动

本公司的主要控制措施包括:

1．不相容职务分离控制

公司在岗位设置前会对各业务流程中所涉及的不相容职务进行分析、梳理，考虑到不相容职务分离的控制要求，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制。

2．授权审批控制

公司各项需审批业务有明确的审批权限及流程，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。公司及各控股公司的日常审批业务通过在信息化平台上进行自动控制以保证授权审批控制的效率和效果。

3．会计系统控制

公司严格执行国家统一的会计准则制度，加强会计基础工作，制定了《万科集团会计管理及核算规范》，明确了会计凭证、会计账簿和财务会计报告的处理程序。公司的核算工作基本实现了信息化处理，为会计信息及资料的真实完整提供了良好保证。

4．财产保护控制

公司建立了财产日常管理制度和定期清查制度，各项实物资产建立台账进行记录、保管，坚持进行定期盘点及账实核对等措施，以保障公司财产安全。

5．预算控制

公司通过编制营运计划及成本费用预算等实施预算管理控制，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，并通过对营运计划的动态管理强化预算约束，评估预算的执行效果。

6．运营分析控制

公司建立了运营情况分析制度，并通过运营管理平台，实现了对公司运营的信息化管理。公司经理层通过月度经营例会、总裁办公会等形式，定期开展运营情况分析，发现存在问题，及时调整经营策略。

7．绩效考评控制

公司实施以均衡计分卡（BSC）为核心的组织绩效管理，从财务、顾客、内部运作和学习成长四个维度出发制定考核方案并据此对总部、区域本部和子公司进行考核。公司每年组织季度考核、年度考核，考核结果将作为奖金分配、甄选与培养、团队优化、薪金福利调整等工作提供依据。

公司将上述控制措施在下列主要业务活动中综合运用，对各种业务及事项实施有效控制，促进内部控制有效运行。

1．销售

2009 年度，公司梳理及细化了市场营销部对销售相关业务的管控职责，制定及修订了包括《万科集团营销费用分类管理规范》、《项目开盘认购的操作指引》、《明源销售系统使用规范》等在内的销售管理制度，遵循合约明晰、授权审批和不相容职务相分离的原则，使用销售管理平台对项目定价、认购、折扣、签约、回款等业务进行控制和记录。细化了对销售收款等高风险环节的控制流程，加强了对销售费用管理的控制力度。实际业务控制中，所有业务操作均需履行公司设定的审批流程，其中重大和关键业务操作必须在得到子公司管理层的审批后方加以实施。同时制度体系中也设计了复核、检查监督机制，完善对业务操作的管控。

2．成本

公司主要由工程采购与成本管理部负责对成本相关流程的管控，本年修订了包括《万科集团房地产开发企业成本核算指导》、《万科集团工程款

支付管理规定》等在内的成本管理制度，实施成本对标管理，持续进行成本优化。使用成本管理软件，对项目运作全过程成本信息进行计划管理和动态跟踪记录。项目确定后，子公司按公司总部统一要求编制项目目标成本（成本计划），经公司管理层和区域成本管理部门审批确认后执行，同时录入集团成本管理系统。项目开发过程中，已发生成本由专人负责及时录入成本软件，同时成本管理部门定期对待发生成本做出预测，并在必要时进行调整，从而对项目成本形成动态跟踪管理。子公司财务管理部门负责项目动态成本中的非合同费用录入。此外，通过定期的成本清查工作，保障子公司动态成本数据准确性，总部与区域通过开展成本检查等工作对子公司成本信息反映的及时性和准确性进行监督。

3．资金

公司本年已经制定及修订了包括《万科集团资金管理制度》、《万科集团资金结算操作规范》等，明确公司资金管理、结算的要求，对资金业务进行管理和控制，从而降低资金使用成本并保证资金安全。总部设立资金管理中心，对公司和各子公司的融资和结算业务实行统一管理。子公司银行账户开销户均需得到资金管理中心的审批确认；融资业务由资金管理中心统一管理，子公司对外进行融资，须在资金管理中心统一安排下，经审批后进行；付款方面，主要经营付款亦由资金管理中心进行统一结算。同时，资金管理中心还通过定期编制年度资金计划和月度动态滚动资金计划强调资金管理的计划性，并对子公司的资金计划完成情况进行跟踪，实时调整资金安排。

4．采购

公司主要由工程采购与成本管理部负责对采购业务的管控，本年度公司已制定及修订了包括《工程采购实施细则》、《供应商管理细则》等在内

的采购管理制度，规范采购业务操作，加强集中采购、推行战略合作等采购模式和招投标、竞争性谈判等多种采购方式，兼顾采购的效益、效率和规范性，并使用采购管理平台提升采购的效率和透明度。通过招投标方式，严格进行经济标和技术标评审，在公平公正、充分竞争的基础上择优选择供应商，保证采购成本和质量的合理性；通过集中采购，整合内部需求和外部资源，最大限度发挥采购量的优势以实现规模效益；通过战略合作，在对关键产品/服务供应商进行全面评估的基础上，与评价为最优的供应商建立长期、紧密、稳定的合作关系，以达到最优采购绩效；公司各子公司均使用采购平台，有效提高了采购效率和透明度。在采购付款环节，加强了支付环节的核对和审查及对供应商的后评估，以保证付款的准确性及合理性。

5．重大投资

公司投资业务主要由战略与投资管理部负责管控，公司已经制定及修订了包括《万科集团新项目发展制度》、《万科集团新项目投资工作指引》等在内的投资管理制度，并使用新项目决策平台对重大投资进行管理。本年度，公司始终坚持“精挑细选”的策略，重点考虑价格的合理性和风险的可控性，严格评估项目收益的可行性，通过严格的分级授权审批程序对重大投资实施全程监控。公司对投资实行区域本部审查、总部决策的控制模式，区域子公司的投资项目，除重大战略并购外，其余均由区域本部进行项目初步审查，经总部相关专业部门联合评审后，报由公司管理层组成的投资与决策委员会在董事会授权范围内进行决策；公司重大战略并购投资以及非区域子公司的投资项目，经公司相关专业部门联合评审后，由投资与决策委员会直接在董事会授权范围内进行决策。项目投资金额超过公司董事会对公司授权的，需在报董事会决议通过后方可实施。

6．对子公司的管理

公司构建总部、区域、一线的三级架构体系。在三级架构体系下，总部对区域本部和子公司的授权和职责划分坚持不相容职责相分离的原则；总部专业部门统一制定制度，对一线公司进行专业指导；并通过内部审计、专业检查、监事巡查等手段，检查、监督公司各层级职责的有效履行。

（1）公司已经制定《万科集团法人事项管理办法》等制度，规范各子公司设立及注销等业务的控制流程。对于超过公司董事会授权范围的子公司设立、对外转让股权、子公司解散清算等，除履行公司内审批程序外，还需报公司董事会审议通过后方加以实施；对于公司董事会授权公司管理层进行决策的法人事项则在管理层进行决策后，报董事会备案。

（2）重大事项报告与审议方面，建立统一规范的报告渠道和方式。公司制定发布了《万科集团信息管理办法》，建立了包括经营管理例会、总裁办公会等在内的定期、不定期专题办公会议制度，以把握集团的整体经营状况，并决策重大经营管理事项。子公司定期向总部上报各类经营信息，对临时重大事项，即时向区域或总部相关职能部门专项报告。

（3）财务核算管理方面，总部财务管理部制定及修订了包括《万科集团会计管理及核算规范》、《万科集团内部往来、内部交易核算规范》等制度，指导控股公司的财务核算工作。财务报告期末，各控股公司须按照总部财务管理部发布的“结算通知”要求报送财务报表，并由总部财务管理部对各控股公司的核算质量进行考核。

（4）对于新并购的子公司，公司加强业务整合的同时，还通过内部培训和企业文化宣讲，加快企业融合进程；通过应用公司统一使用的信息系统平台，实现内部信息及时传递。

7．关联交易

公司对关联交易采取公平、公正、自愿、诚信以及对公司有利的原则，关联交易定价按照公平市场价格，充分保护各方投资者的利益，必要时聘请独立财务顾问或专业评估师对其进行评价并按规定披露。根据《深圳证券交易所股票上市规则》和《公司章程》的相关规定，公司明确划分股东大会和董事会对关联交易的审批权限。重大关联交易在经独立董事认可后，方提交董事会审议。披露关联交易时，同时披露独立董事的意见。

8．对外担保

按照证监会《关于规范上市公司对外担保行为的通知》、《深圳证券交易所股票上市规则》等相关规定，公司制定了《万科企业股份有限公司担保管理制度》，明确规定担保业务评审、批准、执行等环节的控制要求，对担保业务进行控制。原则上公司除因住宅销售业务对部分业主提供按揭担保外，不对外（非关联公司）提供担保，由于并购业务发生无法避免的担保业务时，均履行必要的内部审批程序，并提请公司董事会审议通过，特定担保事项则在提交股东大会审议通过后，方予以实施。对外提供的担保在必要时要求被担保方提供反担保，以规避由担保可能给公司造成的损失。公司所有担保事项由总部统一控制并做后续管理，限制控股子公司提供担保。

9．募集资金使用

公司制定《万科企业股份有限公司募集资金管理办法》，严格按照《中华人民共和国公司法》、《中华人民共和国证券法》、《上市公司证券发行管理办法》等法律法规的相关规定对募集资金进行管理，公司对募集资金采取了专户存储、专款专用的原则，由总部资金中心进行统一管理，并聘请外部审计师对募集资金存放和使用情况进行审计，审计结果和投资项目进

展情况在定期报告中予以披露。

10．信息披露

公司根据《中华人民共和国公司法》、《中华人民共和国证券法》、《深圳证券交易所上市规则》、《公司章程》等的有关规定，制定了《万科企业股份有限公司信息披露管理办法》，通过分级审批控制保证各类信息以适当的方式及时准确完整地向外部信息使用者传递。公司董事会办公室负责对监管部门披露要求的及时获取及实时跟踪。公司公开披露的信息文稿由董事会办公室负责起草，由董事会秘书进行审核，在履行法定审批程序后加以披露。公司选择《中国证券报》、《上海证券报》、《证券时报》、巨潮资讯网站等媒体作为公开信息披露的渠道，所披露的任何信息均首先在上述指定媒体披露。公司董事会办公室设专人负责回答投资者所提的各种关于万科的问题，相关人员以公开披露的信息作为回答投资者提问的依据。同时通过公司外部网络中的投资者关系栏目及时公布相关信息，与更广大的投资者进行广泛交流。

公司相关制度规定，信息披露相关当事人对所披露的信息负有保密义务，在未对外公开披露前不得以任何方式向外界透露相关内容。公司对所披露信息的解释由董事会秘书执行，其他当事人在得到董事会授权后可对所披露信息的实际情况进行说明。董事会办公室根据信息披露需要在全公司范围内收集相关信息，在该等信息未公开披露前，所有相关人员均应履行保密职责，凡违反信息披露要求的，对相关责任人给予批评、警告处罚，情节严重的给予行政和经济处分，并视情形追究法律责任。

五、信息与沟通

公司已经制定出包括《万科集团信息管理办法》、《万科集团信息保密制度》、《集团总部会议管理规定》等在内的各项制度，规范公司内经营信

息传递秩序。日常经营过程中，建立了定期与不定期的业务与管理快报、专项报告等信息沟通制度，便于全面及时了解公司经营信息，并通过各种例会、办公会等方式管理决策，保证公司的有效运作。

公司持续地运用信息化手段提高管理决策及运营效力，流程与信息管理部作为信息化工作的执行及管理机构，负责公司财务系统、业务运营系统和办公管理系统的规划、开发与管理，负责组织公司各类信息系统的开发与维护，在全公司范围内提供信息系统共享服务。建设了万科信息安全管理体系，制定了一系列信息安全方针、策略和制度，保护公司的信息资产，积极预防安全事件的发生。公司还将持续优化信息流程并进行信息系统的整合。

在与客户、合作伙伴、投资者和员工关系方面，公司已建立起较完整透明的沟通渠道，在完善沟通的同时发挥了对公司管理的监督作用。对客户，公司本着“与客户一起成长，让万科在投诉中完美”的客户理念，设立五条投诉沟通渠道，与客户进行良性互动；对投资者，公司除了通过法定信息披露渠道发布公司信息外，投资者还可以通过电话、电子邮件、访问公司网站、直接到访公司、参与公司组织的网络路演和见面会等方式了解公司信息，公司建立网络辅助系统及时响应投资者的各类需求，保证投资者及时了解公司的经营动态，通过互动加强对公司的理解和信任；对员工，设立十二条沟通渠道，保证沟通顺畅有效；对合作伙伴，倡导合作共生共赢，通过多种渠道定期沟通等多种渠道，保持良好的合作关系。

六、内部监督

公司已经建立起涵盖总部、区域、一线三个层面的监督检查体系，审计部、风险管理部、总部其他职能部门或聘请的第三方对各业务领域的控制执行情况进行定期与不定期的专项检查及评估，保证控制活动的存在并

有效运行。监事会执行内部反舞弊职能，建立定期对各子公司的巡查机制，并负责归口处理实名与匿名投诉事宜，有效发挥其监督作用。

七、重点控制活动中的问题及整改计划

通过公司自我评价及整改，截至2009年12月31日，本公司内部控制体系基本健全，未发现对公司治理、经营管理及发展有重大影响之缺陷及异常事项。

八、内部控制自我评价结论

董事会认为，公司已经建立起的内部控制体系在完整性、合规性、有效性等方面不存在重大缺陷。但由于内部控制固有的局限性、内部环境以及宏观环境、政策法规持续变化，可能导致原有控制活动不适用或出现偏差，对此公司将及时进行内部控制体系的补充和完善，为财务报告的真实性、完整性，以及公司战略、经营等目标的实现提供合理保障。

万科企业股份有限公司

董事会

二〇一〇年二月二十六日

附录A

企业内部控制评价指引（征求意见稿）

第一章　总则

第一条　为了规范企业内部控制评价，全面评估内部控制设计与运行情况，编制内部控制评价报告，根据有关法律法规和《企业内部控制基本规范》，制定本指引。

第二条　本指引所称内部控制评价，是指企业董事会（或类似决策机构）或其授权机构，对内部控制设计与运行的有效性进行综合评估的过程。

第三条　企业应当根据《企业内部控制基本规范》和本评价指引，结合本企业的实际情况，制定内部控制评价办法，明确内部控制评价的原则和内容、程序和方法，以及报告形式等相关内容，确保内部控制评价工作落到实处。

企业主要负责人应当对内部控制评价结论的真实性负责。

第四条　企业应当建立内部控制评价结果分析利用和考核制度，将内部控制评价结果和整改情况作为内部绩效考评的重要依据。



第二章 评价的原则和内容

第五条 企业实施内部控制评价，至少应当遵循全面性、重要性和独立性原则，确保评价工作标准统一、客观公正。

全面性，是指评价工作应当包括内部控制的设计与运行，涵盖企业及其所属单位的各种业务和事项。

重要性，是指在全面评价的基础上关注重要高风险领域。

独立性，是指评价工作应当与内部控制的设计与运行相互分离。

第六条 企业内部控制评价应当以内部环境为基础，重点关注：治理结构是否形同虚设；发展战略是否可行；机构设置是否重叠；权责分配是否明晰；不相容岗位是否分离；人力资源政策和激励约束机制是否科学合理；企业文化是否促进员工勤勉尽责；社会责任是否有效履行等。

第七条 企业内部控制评价应当以生产经营活动为重点，至少关注：资金的筹集、投放和营运过程是否存在资金链断裂；资产运行中是否存在效能低下或资产流失；采购与销售环节是否存在舞弊行为；研发项目是否经过科学论证；工程项目是否存在商业贿赂等。

第八条 企业内部控制评价应当兼顾控制手段，至少关注：全面预算是否具有约束力；合同履行是否存在纠纷；信息系统是否与内部控制有机结合；内部报告是否及时传递和有效沟通等。

第三章 评价的程序和方法

第九条 企业应当指定内部审计机构或其他机构具体组织实施内部控制评价工作，根据内部控制评价办法制定评价方案，组成评价小组，明确分工和进度安排，采取现场检查等方式开展内部控制评价。

企业可以借助中介机构或外部专家实施内部控制评价，参与企业内部

控制评价的中介机构不得同时为同一企业提供内部控制审计服务。

第十条　企业开展内部控制评价，应当编制工作底稿。工作底稿应当由评价小组直接填写，指定专人严格复核。

第十一条　评价小组可以综合运用个别访谈、调查问卷、专题讨论、穿行测试、统计抽样、比较分析等多种方法，广泛收集被评价单位内部控制设计和有效运行的证据，研究认定内部控制设计缺陷和运行缺陷。

评价小组研究认定的内部控制缺陷，应当按照规定的权限和程序报经审批后确定。

第十二条　企业应当对内部控制缺陷进行综合判断，按其严重程度分为重大缺陷、重要缺陷和一般缺陷。

重大缺陷，是指一个或多个控制缺陷的组合，可能导致企业严重偏离控制目标的情形。

重要缺陷，是指一个或多个控制缺陷的组合，其严重程度和经济后果低于重大缺陷，但仍有可能导致企业偏离控制目标的情形。

一般缺陷，是指除重大缺陷、重要缺陷之外的其他控制缺陷。

第十三条　重大缺陷应当根据本指引第五条、第六条、第七条规定和重大缺陷的定义，结合企业实际情况，具体加以认定。

重要缺陷和一般缺陷由企业自行确定。

第十四条　企业应当建立内部控制缺陷整改机制，明确内部各管理层级和单位整改的职责分工，确保内部控制设计与运行中的主要问题和重大风险得到及时解决和有效控制。

董事会负责重大缺陷的整改，接受监事会的监督。经理层负责重要缺陷的整改，接受董事会的监督。内部有关单位负责一般缺陷的整改，接受经理层的监督。

第四章　内部控制评价报告

第十五条　企业应当根据内部控制评价结果和整改情况，编制内部控制评价报告。内部控制评价报告至少应当包括下列内容：

（一）组织实施内部控制评价的总体情况。

（二）内部控制责任主体的声明。

（三）内部控制评价的范围和内容。

（四）内部控制评价的标准和依据。

（五）内部控制评价的程序和方法。

（六）内部控制重大缺陷及其认定情况。

（七）内部控制重大缺陷的整改措施及责任追究情况。

（八）内部控制有效性的结论。

存在一个或多个内部控制重大缺陷的，应当做出内部控制无效的结论。

第十六条　企业内部控制评价报告应当报企业经理层审核、董事会审定后公布。

第十七条　企业应当以 12 月 31 日作为年度内部控制评价报告的基准日，也可选择 6 月 30 日为基准日。内部控制评价报告应于基准日后 4 个月内报出。

附录B
企业内部控制审计指引（征求意见稿）

第一章　总则

第一条　为了规范注册会计师执行企业内部控制审计业务，明确工作要求，保证执业质量，根据《中国注册会计师鉴证业务基本准则》及相关执业准则，制定本指引。

第二条　本指引所称内部控制审计，是指会计师事务所接受委托，对截至特定日期企业内部控制的有效性进行审计，并发表审计意见。

本指引中内部控制审计的范围，主要是企业为了合理保证财务报告及相关信息真实完整、资产安全而设计和执行的内部控制。用以合理保证资产安全的内部控制，可能涉及合理保证经营效率和效果、经营管理合法合规的内部控制。

注册会计师在内部控制审计或财务报表审计中实施的程序并不是企业内部控制的组成部分。

第三条　在企业治理层的监督下，按照《企业内部控制基本规范》和相关规定，设计、实施和维护有效的内部控制，并评价其有效性是企业管理层的责任。按照本指引的要求，在实施审计工作的基础上对内部控制的

有效性发表审计意见，是注册会计师的责任。

内部控制审计不能减轻企业管理层的责任。

第四条　有效的内部控制能够为财务报告及相关信息真实完整、资产安全提供合理保证。

如果存在一项或多项重大缺陷，内部控制应被认定为无效。

即使财务报表不存在重大错报，内部控制也可能存在重大缺陷。

第五条　注册会计师应当计划和实施审计工作，获取充分、适当的证据，为截至特定日期内部控制是否不存在重大缺陷提供合理保证，并作为支持审计意见的基础。

第二章　整合审计

第六条　注册会计师应当将内部控制审计与财务报表审计整合进行（以下简称整合审计）。

内部控制审计和财务报表审计的目标不同。注册会计师应当计划和实施审计工作，以同时实现两者的目标。

第七条　在整合审计中，注册会计师应当计划和实施对控制设计和运行有效性的测试，以同时实现下列目标：

（一）获取充分、适当的证据，支持其在内部控制审计中对内部控制的有效性发表的意见；

（二）获取充分、适当的证据，支持其在财务报表审计中对内部控制的风险评估结果。

第三章　计划审计工作

第一节　总体要求

第八条　注册会计师应当恰当地计划内部控制审计工作，并对助理人

员进行适当的督导。

第九条　在计划整合审计工作时，注册会计师应当评价下列事项对财务报表和内部控制是否有重要影响，以及有重要影响的事项将如何影响审计工作：

（一）注册会计师执行其他业务时了解的情况；

（二）在评价是否接受与保持客户和业务时，注册会计师了解的与企业相关的风险情况；

（三）影响企业所处行业的事项，如行业财务报告惯例、经济状况和技术革新；

（四）与企业相关的法律法规；

（五）与企业经营相关的重要事项，包括组织结构、经营特征和资本结构；

（六）经营活动的复杂程度；

（七）经营活动或内部控制最近发生变化的程度；

（八）注册会计师对重要性、风险以及与确定内部控制重大缺陷相关的其他因素所作的初步判断；

（九）以前与审计委员会或管理层沟通过的控制缺陷；

（十）可获取的、与内部控制有效性相关的证据的类型和范围；

（十一）对内部控制有效性的初步判断；

（十二）与评价财务报表发生重大错报的可能性和内部控制有效性相关的公开信息。

第二节　风险评估的作用

第十条　在内部控制审计中，注册会计师应当以风险评估为基础，确定重要账户、列报及其相关认定，选择拟测试的控制，以及确定针对特定

控制所需收集的证据。

第十一条　内部控制的特定领域存在重大缺陷的风险越高，给予该领域的审计关注就越多。

注册会计师应当更多地关注高风险领域，而没有必要测试那些即使有缺陷、也不可能导致财务报表重大错报的控制。

第十二条　在进行风险评估以及确定审计程序时，注册会计师应当考虑企业组织结构、经营流程或业务单元的复杂程度可能产生的重要影响。

第三节　调整审计工作

第十三条　企业组织结构、经营流程及业务单元的规模和复杂程度影响许多控制目标的实现方式。注册会计师应当根据企业具体情况调整审计工作，以获取充分、适当的证据，支持发表的审计意见。

第四节　应对舞弊风险

第十四条　在计划和实施内部控制审计工作时，注册会计师应当考虑财务报表审计中对舞弊风险的评估结果。在识别和测试企业层面控制以及选择其他控制进行测试时，注册会计师应当评价企业的控制是否足以应对已识别的、由舞弊导致的重大错报风险，并评价为应对管理层凌驾于控制之上的风险而设计的控制。

第十五条　在内部控制审计中，如果识别出旨在防止或发现舞弊的控制存在缺陷，注册会计师在财务报表审计中应当按照《中国注册会计师审计准则第 1141 号——财务报表审计中对舞弊的考虑》的规定，在制定应对重大错报风险的方案时考虑这些缺陷。

第五节　利用其他相关人员的工作

第十六条　注册会计师应当评估是否利用他人（包括企业的内部审计人员、其他人员以及在管理层或审计委员会指导下的第三方）的工作以及

利用的程度，以减少可能本应由注册会计师执行的工作。

如果决定利用内部审计人员的工作，注册会计师应当按照《中国注册会计师审计准则第 1411 号——考虑内部审计工作》的规定办理。

第十七条　如果拟利用他人的工作，注册会计师应当评价该人员的专业胜任能力和客观性，以确定可利用程度。

第十八条　在内部控制审计中，注册会计师利用他人工作的程度还受到与被测试控制相关的风险的影响。与某项控制相关的风险越高，可利用他人工作的程度就越低，注册会计师应当越多地亲自对该项控制进行测试。

第十九条　如果其他注册会计师负责审计企业的一个或多个分部、分支机构、子公司等组成部分的财务报表和内部控制，注册会计师应当按照《中国注册会计师审计准则第 1401 号——利用其他注册会计师的工作》的规定，确定自己能否担任主审注册会计师，以及是否利用其他注册会计师的工作。

第六节　确定重要性水平

第二十条　在计划内部控制审计工作时，注册会计师应当使用与财务报表审计相同的重要性水平。

第七节　对企业使用服务机构的考虑

第二十一条　在内部控制审计中，如果服务机构执行企业的交易，并履行受托责任，该服务机构的服务可能影响企业的内部控制。在这种情况下，注册会计师应当按照《中国注册会计师审计准则第 1212 号——对被审计单位使用服务机构的考虑》的规定办理。

第四章　实施审计工作

第一节　总体要求

第二十二条　管理层实施的内部控制评价应当以控制环境（也称内部环境）为基础，以生产经营活动为重点，并兼顾控制手段。相应的，在内部控制审计中，注册会计师应当以风险评估为基础，运用自上而下的方法，选择拟测试的控制。

第二十三条　自上而下的方法按照下列思路展开：

（一）从财务报表层次初步了解内部控制整体风险；

（二）识别企业层面控制；

（三）识别重要账户、列报及其相关认定；

（四）了解错报的可能来源；

（五）选择拟测试的控制。

自上而下的方法是注册会计师识别风险、选择拟测试的控制的思路，但并不一定是实施审计工作的顺序。

第二节　识别企业层面控制

第二十四条　注册会计师应当测试对评价内部控制有效性有重要影响的企业层面控制。对企业层面控制的评价，可能增加或减少本应对其他控制进行的测试。

第二十五条　企业层面控制包括：

（一）与控制环境相关的控制；

（二）针对管理层凌驾于控制之上的风险而设计的控制；

（三）企业的风险评估过程；

（四）集中化的处理和控制，包括共享的服务环境；

（五）监控经营成果的控制；

（六）监督其他控制的控制，包括内部审计职能、审计委员会的活动及内部控制自我评价；

（七）对期末财务报告流程的控制；

（八）针对重大经营控制及风险管理实务而采取的政策。

第二十六条　控制环境对保持有效的内部控制有重要影响，注册会计师应当评价企业的控制环境。

第二十七条　期末财务报告流程对内部控制审计和财务报表审计有重要影响，注册会计师应当评价期末财务报告流程。

期末财务报告流程包括：

（一）将交易总额登入总分类账的程序；

（二）与会计政策的选择和运用相关的程序；

（三）总分类账中会计分录的编制、批准等处理程序；

（四）对财务报表进行调整的程序；

（五）编制财务报表的程序。

由于期末财务报告流程通常发生在管理层评价日之后，注册会计师一般只能在该日之后测试相关控制。

第三节　识别重要账户、列报及其相关认定

第二十八条　注册会计师应当识别重要账户、列报及其相关认定。

如果某账户或列报可能包含了一个错报，该错报单独或连同其他错报将对财务报表产生重大影响（需要同时考虑多报和少报的风险），则该账户或列报为重要账户或列报。判断某账户或列报是否为重要账户或列报，应当依据其固有风险，而不应考虑相关控制的影响。

如果某财务报表认定可能包含了一个或多个错报，这个或这些错报将导致财务报表重大错报，则该认定为相关认定。判断某认定是否为相关认

定，应当依据其固有风险，而不应考虑相关控制的影响。

第二十九条　为识别重要账户、列报及其相关认定，注册会计师应当从下列方面评价财务报表项目及附注的错报风险因素：

（一）账户的规模和构成；

（二）易于发生错报的程度；

（三）账户或列报中反映的交易的业务量、复杂性及同质性；

（四）账户或列报的性质；

（五）与账户或列报相关的会计处理及报告的复杂程度；

（六）账户发生损失的风险；

（七）账户或列报中反映的活动引起重大或有负债的可能性；

（八）账户记录中是否涉及关联方交易；

（九）账户或列报的特征与前期相比发生的变化。

第三十条　在识别重要账户、列报及其相关认定时，注册会计师还应当确定对财务报表产生重大影响的潜在错报的可能来源。注册会计师可通过考虑在特定的重要账户或列报中错报可能发生的领域和原因，确定潜在错报的可能来源。

第三十一条　在内部控制审计中，注册会计师在识别重要账户、列报及其相关认定时应当评价的风险因素，与财务报表审计中考虑的因素相同。因此，在这两种审计中识别的重要账户、列报及其相关认定应当相同。

在财务报表审计中，注册会计师可能针对非重要账户、列报及其相关认定实施实质性程序。

第三十二条　如果某潜在重要账户或列报的各组成部分存在的风险差异较大，企业可能采用不同的控制以应对这些风险，注册会计师应当分别处理。

第四节　了解错报的可能来源

第三十三条　注册会计师应当执行下列工作，了解潜在错报的可能来源，以选择拟测试的控制：

（一）了解与相关认定有关的交易的处理流程，包括这些交易如何生成、批准、处理及记录；

（二）验证注册会计师已识别出的、业务流程中可能发生重大错报（尤其是由舞弊导致的错报）的环节；

（三）识别管理层用于应对这些潜在错报的控制；

（四）识别管理层用于及时防止或发现未经授权的、导致财务报表重大错报的资产取得、使用或处置的控制。

第三十四条　注册会计师应当了解信息技术如何影响企业的业务流程。注册会计师应当按照《中国注册会计师审计准则第 1211 号——了解被审计单位及其环境并评估重大错报风险》的规定，考虑信息技术对内部控制及风险评估的影响。

第三十五条　穿行测试通常是完成本指引第三十三条所规定工作的最有效方式。穿行测试是指追踪某笔交易从发生到最终被反映在财务报表中的整个处理过程。

在执行穿行测试时，注册会计师使用的文件和信息技术应当与企业员工使用的相同。

在执行穿行测试时，通常需要综合运用询问适当人员、观察经营活动、检查相关文件及重新执行控制等程序。

第三十六条　在执行穿行测试时，针对特定交易的重要处理环节，注册会计师可以询问企业员工对规定程序及控制的了解程度。这些试探性提问连同穿行测试中的其他程序，可以帮助注册会计师充分了解业务流程，

识别必要控制设计无效或出现缺失的重要环节。

第五节　选择拟测试的控制

第三十七条　注册会计师应当评价控制是否足以应对评估的每个相关认定的错报风险，并选择其中对形成评价结论具有重要影响的控制进行测试。

第三十八条　对特定的相关认定而言，可能有多项控制应对评估的错报风险；反之，一项控制可能应对评估的多个相关认定的错报风险。注册会计师没有必要测试与某个相关认定有关的所有控制。

第三十九条　在确定是否测试某项控制时，不论该项控制的分类和名称如何，注册会计师应当考虑其单独或连同其他控制，是否足以应对评估的某项相关认定的错报风险。

第六节　测试控制设计的有效性

第四十条　注册会计师应当测试控制设计的有效性。

如果某项控制由拥有必要授权和专业胜任能力的人员按规定执行，能够实现控制目标，从而有效防止或发现可能导致财务报表重大错报的错误或舞弊，则表明该项控制的设计是有效的。

第四十一条　注册会计师在测试控制设计的有效性时，应当综合运用询问适当人员、观察经营活动和检查相关文件等程序。

执行穿行测试通常足以评价控制设计的有效性。

第七节　测试控制运行的有效性

第四十二条　注册会计师应当测试控制运行的有效性。

如果某项控制正在按照设计运行、执行人员拥有必要授权和专业胜任能力，则表明该项控制的运行是有效的。

第四十三条　注册会计师在测试控制运行的有效性时，应当综合运用

询问适当人员、观察经营活动、检查相关文件以及重新执行控制等程序。

第八节　风险与拟获取证据的关系

第四十四条　在测试所选定控制的有效性时，注册会计师应当根据与控制相关的风险，确定所需获取的证据。

与控制相关的风险包括控制可能无效的风险和因控制无效而导致重大缺陷的风险。与控制相关的风险越高，注册会计师需要获取的证据就越多。

注册会计师应当针对每一相关认定获取控制有效性的证据，以便对内部控制整体的有效性发表意见，但没有责任对单项控制的有效性发表意见。

第四十五条　得出控制运行无效的结论所需的证据通常比得出其运行有效的结论所需的证据少。

第四十六条　下列因素影响与某项控制相关的风险：

（一）该项控制拟防止或发现的错报的性质和重要程度；

（二）相关账户、列报及其认定的固有风险；

（三）相关账户或列报是否曾经出现错报；

（四）交易的数量和性质是否发生变化，进而可能对该项控制设计或运行的有效性产生不利影响；

（五）企业层面控制（特别是监督其他控制的控制）的有效性；

（六）该项控制的性质及其执行频率；

（七）该项控制对其他控制（如控制环境或信息技术一般控制）有效性的依赖程度；

（八）该项控制的执行或监督人员的专业胜任能力，以及其中的关键人员是否发生变化；

（九）该项控制是人工控制还是自动化控制；

（十）该项控制的复杂程度，以及在运行过程中依赖判断的程度。

第四十七条　如果发现控制偏差，注册会计师应当确定该偏差对相关风险评估、需要获取的证据以及控制运行有效性结论的影响。

第四十八条　注册会计师通过测试控制有效性获取的证据，取决于实施程序的性质、时间和范围的组合。就单项控制而言，注册会计师应当根据与该项控制相关的风险，适当组合实施程序的性质、时间和范围，以获取充分、适当的证据。

第四十九条　注册会计师测试控制有效性实施的程序，按提供证据的效力，由弱到强排序为：询问、观察、检查和重新执行。

询问本身并不能为得出控制是否有效的结论提供充分、适当的证据。

第五十条　测试控制有效性实施的程序，其性质在很大程度上取决于拟测试控制的性质。某些控制可能存在文件记录，反映其运行的有效性，而另外一些控制，如管理理念和经营风格，可能没有书面的运行证据。

对缺乏正式运行证据的企业或业务单元，注册会计师可以通过询问并结合运用观察活动、检查非正式的书面记录和重新执行某些控制，获取有关控制有效性的充分、适当的证据。

第五十一条　对控制有效性的测试涵盖的期间越长，提供的控制有效性的证据越多。

对控制有效性的测试实施的时间越接近管理层评价日，提供的控制有效性的证据越有力。

为获取充分、适当的证据，注册会计师应当在下列两个因素之间做出平衡，以确定测试的时间：

（一）尽量在接近管理层评价日实施测试；

（二）实施的测试需要涵盖足够长的期间。

第五十二条　在管理层评价日之前，管理层可能为提高控制效率、效

果或弥补控制缺陷而改变企业的控制。

如果新控制实现了相关控制目标，运行足够长的时间，且注册会计师能够测试并评价该项控制设计和运行的有效性，则无须测试被取代的控制。

如果被取代控制设计和运行的有效性对控制风险的评估有重大影响，注册会计师应当测试该项控制的有效性。

第五十三条　针对某项控制，测试的范围越大，获取的证据越多。

第五十四条　注册会计师执行内部控制审计业务通常旨在对特定日期（通常为年末）内部控制的有效性发表意见。如果已获取有关控制在期中运行有效性的证据，注册会计师应当确定还需要获取哪些补充证据，以证实在剩余期间控制的运行情况。

第五十五条　在将期中测试的结果更新至年末时，注册会计师应当考虑下列因素，以确定需获取的补充证据：

（一）期中测试的特定控制的有关情况，包括与控制相关的风险、控制的性质和测试的结果；

（二）期中获取的有关证据的充分性、适当性；

（三）剩余期间的长短；

（四）期中测试之后，内部控制发生重大变化的可能性。

第九节　连续审计时的特殊考虑

第五十六条　在连续审计中，注册会计师在确定测试的性质、时间和范围时，应当考虑以前年度执行内部控制审计时了解的情况。

第五十七条　除本指引第四十六条所列因素之外，下列因素也会影响连续审计中与某项控制相关的风险：

（一）以前年度审计中所实施程序的性质、时间和范围；

（二）以前年度对控制的测试结果；

（三）上次审计之后，控制或其运行流程是否发生变化。

第五十八条　在考虑本指引第四十六条和第五十七条所列的风险因素，以及连续审计中可获取的进一步信息之后，只有当认为与控制相关的风险水平比以前年度有所下降时，注册会计师在本年度审计中才可以减少测试。

第五十九条　在连续审计中，由于完全自动化的应用控制通常不会因人为失误而失效，因此，注册会计师可以考虑对自动化应用控制实施对标策略。

第六十条　如果认为程序变更、访问权限及计算机操作方面的一般控制有效，且可持续对其进行测试，并能证实自动化应用控制自最近一次测试之后未发生变化，注册会计师不必重复执行测试，就可以认为自动化应用控制是持续有效的。

注册会计师为证实控制未发生变化而需获取证据的性质和范围，可能随情况的变化而变化。例如，企业程序变更控制的强弱将影响需获取证据的性质和范围。

第五章　评价识别的控制缺陷

第一节　评价控制缺陷的严重程度

第六十一条　如果控制的设计或运行不能使管理层或员工在正常履行职责的过程中及时防止或发现错报，则表明内部控制存在缺陷。

内部控制存在的缺陷包括设计缺陷和运行缺陷。

设计缺陷是指缺少为实现控制目标所必需的控制，或者现有控制设计不适当，即使正常运行也难以实现控制目标。

运行缺陷是指设计适当的控制没有按设计意图运行，或者执行人员缺

乏必要授权或专业胜任能力，无法有效实施控制。

第六十二条　内部控制存在的缺陷，按严重程度分为重大缺陷、重要缺陷和一般缺陷。

重大缺陷是内部控制中存在的、可能导致财务报表重大错报的一项控制缺陷或多项控制缺陷的组合。

重要缺陷是内部控制中存在的、其严重程度不如重大缺陷，但足以引起企业财务报告监督人员关注的一项控制缺陷或多项控制缺陷的组合。

一般缺陷是内部控制中存在的、除重大缺陷和重要缺陷之外的控制缺陷。

第六十三条　注册会计师应当评价其注意到的各项控制缺陷的严重程度，以确定这些缺陷单独或组合起来，是否构成重大缺陷。但是，在计划和实施审计工作时，不要求注册会计师寻找单独或组合起来不构成重大缺陷的控制缺陷。

第六十四条　控制缺陷的严重程度取决于：

（一）控制缺陷导致账户余额或列报错报的可能性；

（二）因一项控制缺陷或多项控制缺陷的组合导致潜在错报的金额大小。

第六十五条　控制缺陷的严重程度与账户余额或列报是否发生错报无关，而取决于控制缺陷是否可能导致错报。

第六十六条　在评价一项控制缺陷或多项控制缺陷的组合是否可能导致账户余额或列报错报时，注册会计师应当考虑的风险因素包括：

（一）所涉及的账户、列报及其相关认定的性质；

（二）相关资产或负债易于发生损失或舞弊的程度；

（三）确定相关金额时所需判断的主观程度、复杂程度及范围；

（四）所涉及的控制与其他控制的相互作用或关系；

（五）控制缺陷之间的相互作用；

（六）控制缺陷在未来可能产生的影响。

第六十七条　在评价因一项控制缺陷或多项控制缺陷的组合导致潜在错报的金额大小时，注册会计师应当考虑的因素包括：

（一）受控制缺陷影响的财务报表金额或交易总额；

（二）在本期或预计的未来期间受控制缺陷影响的账户余额或各类交易涉及的交易量。

第六十八条　在确定一项控制缺陷或多项控制缺陷的组合是否构成重大缺陷时，注册会计师应当评价补偿性控制的影响。为减弱控制缺陷的不利影响，企业执行的补偿性控制应当有足够的精确度，以防止或发现可能发生的重大错报。

第二节　表明可能存在重大缺陷的迹象

第六十九条　下列迹象可能表明内部控制存在重大缺陷：

（一）注册会计师发现高级管理人员舞弊；

（二）企业重述以前公布的财务报表，以更正重大错报；

（三）注册会计师发现当期财务报表存在重大错报，而控制未能发现；

（四）审计委员会对财务报告及内部控制的监督无效。

第七十条　如果注册会计师确定，发现的一项控制缺陷或多项控制缺陷的组合，将导致审慎的管理人员在执行工作时认为自身无法合理保证按照企业会计准则的规定记录交易，应当将这种情况视为内部控制存在重大缺陷的迹象。

第六章　完成审计工作

第一节　形成审计意见

第七十一条　注册会计师应当评价从各种来源获取的证据，包括对控制的测试结果、财务报表审计中发现的错报以及已识别的所有控制缺陷，以形成对内部控制有效性的意见。

第七十二条　在对内部控制的有效性形成意见后，注册会计师应当评价，管理层内部控制评价报告中对与财务报告及相关信息的真实完整、资产安全相关的内部控制的表达是否符合有关法律法规的要求。

如果认为上述表达不完整或不恰当，注册会计师应当按照本指引第九十八条的要求进行处理。

第七十三条　只有在审计范围没有受到限制时，注册会计师才能对内部控制的有效性形成意见。如果存在范围限制，注册会计师应当按照本指引第九十九条至第一百零二条的要求进行处理。

第二节　获取管理层书面声明

第七十四条　注册会计师应当向管理层获取书面声明。管理层声明的内容应当包括：

（一）管理层认可其对设计、实施和维护有效的内部控制负责；

（二）管理层已对内部控制的有效性做出评价，并说明评价时采用的标准；

（三）管理层没有利用注册会计师在内部控制审计和财务报表审计中执行的程序及其结果，作为管理层自我评价的基础；

（四）管理层根据控制标准评价内部控制有效性得出的结论；

（五）管理层已向注册会计师披露识别出的、内部控制在设计或运行方面存在的所有缺陷，并已专门向注册会计师披露所有重要缺陷或重大缺陷；

（六）导致财务报表重大错报的所有舞弊，以及不会导致财务报表重大错报，但涉及管理层和其他在内部控制中具有重要作用的员工的所有舞弊；

（七）注册会计师在以前年度审计中识别的、已与审计委员会沟通的控制缺陷是否已经得到解决，以及哪些缺陷尚未得到解决；

（八）在审计报告日后，内部控制是否发生变化，或者是否存在对内部控制产生重要影响的其他因素，如管理层针对重要缺陷和重大缺陷采取的所有纠正措施。

第七十五条　如果管理层拒绝提供书面声明，或因其他原因未能获取书面声明，注册会计师应当将其视为审计范围受到限制，解除业务约定或出具无法表示意见的审计报告。

注册会计师应当评价，管理层拒绝提供书面声明对其他声明（包括在财务报表审计中获取的声明）的可靠性产生的影响。

第七十六条　注册会计师应当按照《中国注册会计师审计准则第 1341 号——管理层声明》的规定，确定声明书的签署者、声明书涵盖的期间以及何时获取更新的声明书等。

第三节　沟通相关事项

第七十七条　注册会计师应当以书面形式与管理层和审计委员会沟通审计过程中识别的所有重大缺陷。书面沟通应当在注册会计师出具内部控制审计报告之前进行。

第七十八条　如果认为审计委员会对财务报告及其内部控制的监督无效，注册会计师应当就此以书面形式与董事会沟通。

第七十九条　注册会计师应当考虑其识别的一项控制缺陷或多项控制缺陷的组合是否构成重要缺陷。如果构成重要缺陷，则应当就此以书面形式与审计委员会沟通。

第八十条　注册会计师应当以书面形式与管理层沟通其在审计过程中识别的内部控制存在的所有缺陷，并在沟通完成后告知审计委员会。在进行沟通时，注册会计师无须重复自身、内部审计人员或企业其他人员以前书面沟通过的控制缺陷。

第八十一条　本指引不要求注册会计师执行足以识别所有控制缺陷的程序，但是，注册会计师应当沟通其注意到的内部控制的所有缺陷。

第八十二条　如果发现企业存在或可能存在舞弊或违反法规行为，注册会计师应当按照《中国注册会计师审计准则第 1141 号——财务报表审计中对舞弊的考虑》、《中国注册会计师审计准则第 1142 号——财务报表审计中对法律法规的考虑》的规定，确定并履行自身的责任。

第七章　审计报告

第一节　总体要求

第八十三条　注册会计师应当评价根据审计证据得出的结论，以作为对内部控制的有效性形成审计意见的基础。

第八十四条　注册会计师在完成内部控制审计和财务报表审计后，应当分别对内部控制和财务报表出具审计报告。

第二节　标准审计报告

第八十五条　审计报告应当包括下列要素：

（一）标题；

（二）收件人；

（三）引言段；

（四）管理层对内部控制的责任段；

（五）注册会计师的责任段；

（六）内部控制审计的范围段；

（七）内部控制固有局限性的说明段；

（八）内部控制审计意见段；

（九）财务报表审计意见类型的提及段；

（十）注册会计师的签名和盖章；

（十一）会计师事务所的名称、地址及盖章；

（十二）报告日期。

第八十六条　在内部控制审计报告中，财务报表审计意见类型的提及段应当说明，注册会计师还按照中国注册会计师审计准则的规定，审计了企业的财务报表[指出财务报表]，并于××年×月×日出具的审计报告中发表了××意见[指出意见的类型]。如果出具了无法表示意见的财务报表审计报告，应当对该提及段的表述做必要修改。

此外，注册会计师应当在财务报表审计报告意见段后，增加下列段落："我们还按照《企业内部控制审计指引》及相关执业准则的要求，审计了截至××年×月×日企业的内部控制，并在我们出具的××年×月×日（该日期应当与财务报表的审计报告日期一致）的审计报告中，发表了[指出意见的类型]。"如果出具了无法表示意见的内部控制审计报告，应当对该段落的表述做必要修改。

第八十七条　如果符合下列所有条件，注册会计师应当对内部控制出具无保留意见的审计报告：

（一）截至特定日期，企业按照内控规范和相关规定的要求，在所有重大方面保持了有效的内部控制；

（二）注册会计师已经按照《企业内部控制审计指引》的要求计划和实施审计工作，在审计过程中未受到限制。

第八十八条　由于内部控制审计和财务报表审计是整合进行的，注册会计师对内部控制审计报告和财务报表审计报告应当签署相同的日期。

第三节　重大缺陷与非标准审计报告

第八十九条　如果认为内部控制存在一项或多项重大缺陷，除非审计范围受到限制，否则，注册会计师应当对内部控制发表否定意见。

第九十条　注册会计师出具的否定意见审计报告还应包括下列内容：

（一）本指引对重大缺陷的定义；

（二）注册会计师已识别出的重大缺陷（包括在管理层内部控制评价报告中描述的、由管理层识别的内部控制重大缺陷），重大缺陷的性质以及重大缺陷在存在期间对企业编制的财务报表产生的实际和潜在影响等具体情况。

如果重大缺陷尚未包含在管理层内部控制评价报告中，注册会计师应当在审计报告中说明重大缺陷已经识别，但没有包含在管理层内部控制评价报告中。

如果管理层内部控制评价报告中包含了重大缺陷，但注册会计师认为这些重大缺陷未能在所有重大方面得到公允反映，注册会计师应当在审计报告中予以说明，并公允表达有关重大缺陷的必要信息。

第九十一条　如果对内部控制发表否定意见，注册会计师应当确定该意见对财务报表审计意见的影响，并在内部控制审计报告中予以说明。

第四节　期后事项与非标准审计报告

第九十二条　在内部控制审计报告引言段中指出的特定日期之后、审计报告日之前（以下简称期后期间），内部控制可能发生变化，或出现其他可能对内部控制产生重要影响的因素。注册会计师应当向管理层询问是否存在这类变化或影响因素，并按本指引的要求获取管理层关于这些情况的

书面声明。

第九十三条　注册会计师应当针对期后期间，询问并检查下列信息：

（一）在期后期间出具的内部审计报告或类似报告；

（二）其他注册会计师出具的涉及企业内部控制缺陷的报告；

（三）监管机构发布的涉及企业内部控制的报告；

（四）注册会计师在执行其他业务中获取的、有关企业内部控制有效性的信息。

注册会计师还应当考虑获取期后期间的其他文件，并按照《中国注册会计师审计准则第1332号——期后事项》的规定，对其进行检查。

第九十四条　如果知悉对管理层评价日内部控制有效性有重大负面影响的期后事项，注册会计师应当对内部控制发表否定意见。

如果不能确定期后事项对内部控制有效性的影响，注册会计师应当出具无法表示意见的审计报告。

如果管理层在内部控制评价报告中披露了管理层评价日后企业可能采取的纠正措施，注册会计师应当在审计报告中指明不对其发表意见。

第九十五条　注册会计师可能知悉在管理层评价日并不存在，但在期后期间发生的事项。如果这类期后事项对内部控制有重大影响，注册会计师应当在审计报告中增加强调事项段，以描述该事项及其影响，或提醒审计报告使用者关注管理层内部控制评价报告中披露的该事项及其影响。

第九十六条　在出具内部控制审计报告之后，如果知悉在审计报告日已存在的、可能对审计意见产生影响的情况，注册会计师应当按照《中国注册会计师审计准则第1332号——期后事项》的规定办理。

第五节　其他情况与非标准审计报告

第九十七条　如果存在下列情况之一，注册会计师应当出具非标准审

计报告：

（一）管理层内部控制评价报告的表达不完整或不恰当；

（二）审计范围受到限制；

（三）管理层内部控制评价报告中包含其他信息。

第九十八条　如果认为管理层内部控制评价报告的表达不完整或不恰当，注册会计师应当在审计报告中增加强调事项段，说明这一情况并解释得出该结论的理由。如果认为有关内部控制重大缺陷未能在所有重大方面得到公允反映，注册会计师应当按照本指引第九十条的要求进行处理。

第九十九条　注册会计师只有实施了必要的审计程序，才能对内部控制的有效性发表意见。如果审计范围受到限制，注册会计师应当解除业务约定或出具无法表示意见的审计报告。

在出具无法表示意见的审计报告时，注册会计师应当指明无法对内部控制的有效性发表意见。

第一百条　在出具无法表示意见的审计报告时，注册会计师应当在审计报告中说明审计范围不足以支持发表意见，并单设段落说明无法表示意见的实质性理由。注册会计师不应在审计报告中指明所执行的程序，也不应描述内部控制审计的特征，以避免对无法表示意见的误解。

第一百零一条　当拟出具无法表示意见的审计报告时，如果已执行的有限程序发现内部控制存在重大缺陷，注册会计师应当按照本指引第九十条的要求，对重大缺陷做出适当说明。

第一百零二条　如果拟出具无法表示意见的审计报告，注册会计师应当就未能完成整个内部控制审计工作的情况，以书面形式与管理层和审计委员会进行沟通。

第一百零三条　除涉及与财务报告及相关信息的真实完整、资产安全

相关的内部控制信息外，如果管理层内部控制评价报告还包括其他信息，注册会计师应当在审计报告中指明不对其他信息发表意见。

第一百零四条　如果认为其他信息含有对事实的重大错报，注册会计师应当就此与管理层进行讨论。

如果讨论后仍认为存在对事实的重大错报，注册会计师应当以书面形式，将其看法告知管理层和审计委员会。

如果其他信息未包含在管理层内部控制评价报告中，而是包含在年度财务报告中，注册会计师无须在审计报告中指明不对其发表意见。

第八章　审计工作记录

第一百零五条　注册会计师应当按照《中国注册会计师审计准则第1131号——审计工作底稿》的规定，编制内部控制审计工作底稿。

第一百零六条　注册会计师应当就下列内容形成审计工作记录：

（一）制定的内部控制审计计划及重大修改情况；

（二）相关风险评估和选择拟测试控制的主要过程及结果；

（三）测试控制设计和运行有效性的程序及结果；

（四）对识别的控制缺陷的评价；

（五）形成的审计结论和意见；

（六）其他重要事项。

第九章　附则

第一百零七条　本指引自2009年7月1日起施行。

附录 C
内部控制审计报告的参考格式

1. 标准审计报告

内部控制审计报告

××股份有限公司全体股东：

我们审计了截至××年×月×日××股份有限公司（以下简称××公司）的内部控制。

一、管理层对内部控制的责任

在企业治理层的监督下，按照《企业内部控制基本规范》和相关规定，设计、实施和维护有效的内部控制，并评价其有效性是企业管理层的责任。

二、注册会计师的责任

我们的责任是在实施审计工作的基础上对内部控制的有效性发表审计意见。我们按照《企业内部控制审计指引》及相关执业准则的要求执行了审计工作。上述有关规定要求我们遵守职业道德守则，计划和实施审计工作，以对企业在所有重大方面是否保持了有效的内部控制获取合理保证。

审计工作包括获取对内部控制的了解，评估重大缺陷存在的风险，并根据风险评估的结果，测试和评价内部控制设计和运行的有效性。审计工

作还包括实施我们认为必要的其他程序。

我们相信，我们获取的审计证据是充分、适当的，为发表审计意见提供了基础。

三、内部控制审计的范围

本报告中内部控制审计的范围，主要是企业为了合理保证财务报告及相关信息真实完整、资产安全而设计和执行的内部控制。用以合理保证资产安全的内部控制，可能涉及合理保证经营效率和效果、经营管理合法合规的内部控制。

四、内部控制的固有局限性

内部控制具有固有局限性，存在不能防止和发现错报的可能性。此外，由于情况的变化可能导致内部控制变得不恰当，或对控制政策和程序遵循的程度降低，根据内部控制审计结果推测未来内部控制的有效性具有一定风险。

五、内部控制审计意见

我们认为，截至××年×月×日，××公司按照内控规范和相关规定在所有重大方面保持了有效的内部控制。

六、提及财务报表审计意见的类型

我们还按照中国注册会计师审计准则的规定，审计了××公司的财务报表[指出财务报表]，并在××年×月×日出具的审计报告中发表了××意见[指出意见的类型]。

××会计师事务所	中国注册会计师：×××（签名并盖章）
（盖章）	中国注册会计师：×××（签名并盖章）
中国××市	××年×月×日

2. 带强调事项段的无保留意见审计报告

内部控制审计报告

××股份有限公司全体股东：

我们审计了截至××年×月×日××股份有限公司（以下简称××公司）的内部控制。

（“一、管理层对内部控制的责任”至“六、提及财务报表审计意见的类型”参见标准审计报告相关段落表述。）

七、强调事项

我们提醒审计报告使用者关注，[如管理层内部控制评价报告中第×部分第×段所述，××公司发生了一项期后事项。（描述期后事项的性质及其对内部控制的重大影响）]。本段内容不影响已发表的审计意见。

××会计师事务所	中国注册会计师：×××（签名并盖章）
（盖章）	中国注册会计师：×××（签名并盖章）
中国××市	××年×月×日

3. 否定意见审计报告

内部控制审计报告

××股份有限公司全体股东：

我们审计了截至××年×月×日××股份有限公司（以下简称××公司）的内部控制。

（“一、管理层对内部控制的责任”至“四、内部控制的固有局限性”参见标准审计报告相关段落表述。）

五、导致否定意见的事项

重大缺陷是内部控制中存在的、可能导致不能及时防止或发现企业财

务报表重大错报的一项控制缺陷或多项控制缺陷的组合。

[指出注册会计师已识别出的重大缺陷（包括在管理层内部控制评价报告中描述的由管理层识别的内部控制重大缺陷），并说明重大缺陷的性质以及重大缺陷在存在期间对企业编制的财务报表产生的实际和潜在影响等具体情况。]

其中，××重大缺陷没有包含在管理层内部控制评价报告中（如存在这种情况的话，应增加本句）。××重大缺陷虽然已包含在管理层内部控制评价报告中，但未能在所有重大方面得到公允反映，[公允表达有关重大缺陷的必要信息]（如存在这种情况的话，应增加本句）。

有效的内部控制能够为财务报告及相关信息真实完整、资产安全提供合理保证，而上述重大缺陷使××公司内部控制失去这一功能。

（如果上述重大缺陷对财务报表审计意见有影响，说明该影响。）

六、内部控制审计意见

我们认为，由于存在上述重大缺陷及其对实现控制目标的影响，截至××年×月×日，××公司未能按照内控规范和相关规定在所有重大方面保持有效的内部控制。

七、提及财务报表审计意见的类型

（参见标准审计报告相关段落表述。）

××会计师事务所　　　　中国注册会计师：×××（签名并盖章）
（盖章）　　　　中国注册会计师：×××（签名并盖章）
中国××市　　　　××年×月×日

4．无法表示意见审计报告

内部控制审计报告

××股份有限公司全体股东：

我们接受委托，对截至××年×月×日××股份有限公司（以下简称××公司）的内部控制进行审计。

（删除“注册会计师的责任”段，“一、管理层对内部控制的责任”、“二、内部控制审计的范围”和“三、内部控制的固有局限性”参见标准审计报告相关段落表述。）

四、导致无法表示意见的事项

（描述审计范围受到限制的具体情况。）

五、内部控制审计意见

由于审计范围受到上述限制，我们未能实施必要的审计程序以获取发表意见所需的充分、适当证据，因此，我们无法对截至××年×月×日××公司内部控制的有效性发表意见。

六、识别的内部控制重大缺陷（如在审计范围受到限制前，执行有限程序未能识别出重大缺陷，则应删除本段。）

重大缺陷是内部控制中存在的、可能导致不能及时防止或发现企业财务报表重大错报的一项控制缺陷或多项控制缺陷的组合。

[指出注册会计师已识别出的重大缺陷（包括在管理层内部控制评价报告中描述的由管理层识别的内部控制重大缺陷），并说明重大缺陷的性质以及重大缺陷在存在期间对企业编制的财务报表产生的实际和潜在影响等具体情况。]

其中，××重大缺陷没有包含在管理层内部控制评价报告中（如存在这种情况的话，应增加本句）。××重大缺陷虽然已包含在管理层内部控制

评价报告中，但未能在所有重大方面得到公允反映，[公允表达有关重大缺陷的必要信息]（如存在这种情况的话，应增加本句）。

有效的内部控制能够为财务报告及相关信息真实完整、资产安全提供合理保证，而上述重大缺陷使××公司内部控制失去这一功能。

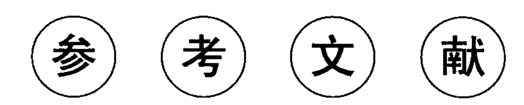
七、提及财务报表审计意见的类型

（参见标准审计报告相关段落表述。）

××会计师事务所　　中国注册会计师：×××（签名并盖章）

（盖章）　　中国注册会计师：×××（签名并盖章）

中国××市　　××年×月×日



参考文献

[1] Sanjay Anand. *Sarbanes-Oxley Guide for Finance and Information Technology Professionals*. New York：John Wiley&Sons，2006.

[2] COSO. 内部控制——整合框架[M]. 方红星，主译. 大连：东北财经大学出版社，2008.

[3] COSO. 企业风险管理——整合框架[M]. 方红星，王宏，译. 大连：东北财经大学出版社，2005.

[4] COSO. 企业风险管理——应用技术[M]. 张宜霞，译. 大连：东北财经大学出版社，2006.

[5] Steven J. Root. 超越 COSO——加强公司治理的内部控制[M]. 刘霄仑，主译. 北京：中信出版社，2004.

[6] 美国管理会计师协会（IMA）. 财务报告内部控制与风险管理[M]. 张先治，袁克利，主译. 大连：东北财经大学出版社，2008.

[7] 杰普・布勒姆. SOX 环境下的 IT 治理[M]. 程治刚，张翎，张劲，译.

大连：东北财经大学出版社，2008.
[8] COSO. 财务报告内部控制：较小型公众公司指南[M]. 方红星，主译. 大连：东北财经大学出版社，2009.
[9] 美国上市公司会计监督委员会（PCAOB）. 第 5 号审计准则—与财务报表审计相结合的财务报告内部控制审计[M]. 张宜霞，主译. 大连：东北财经大学出版社，2008.